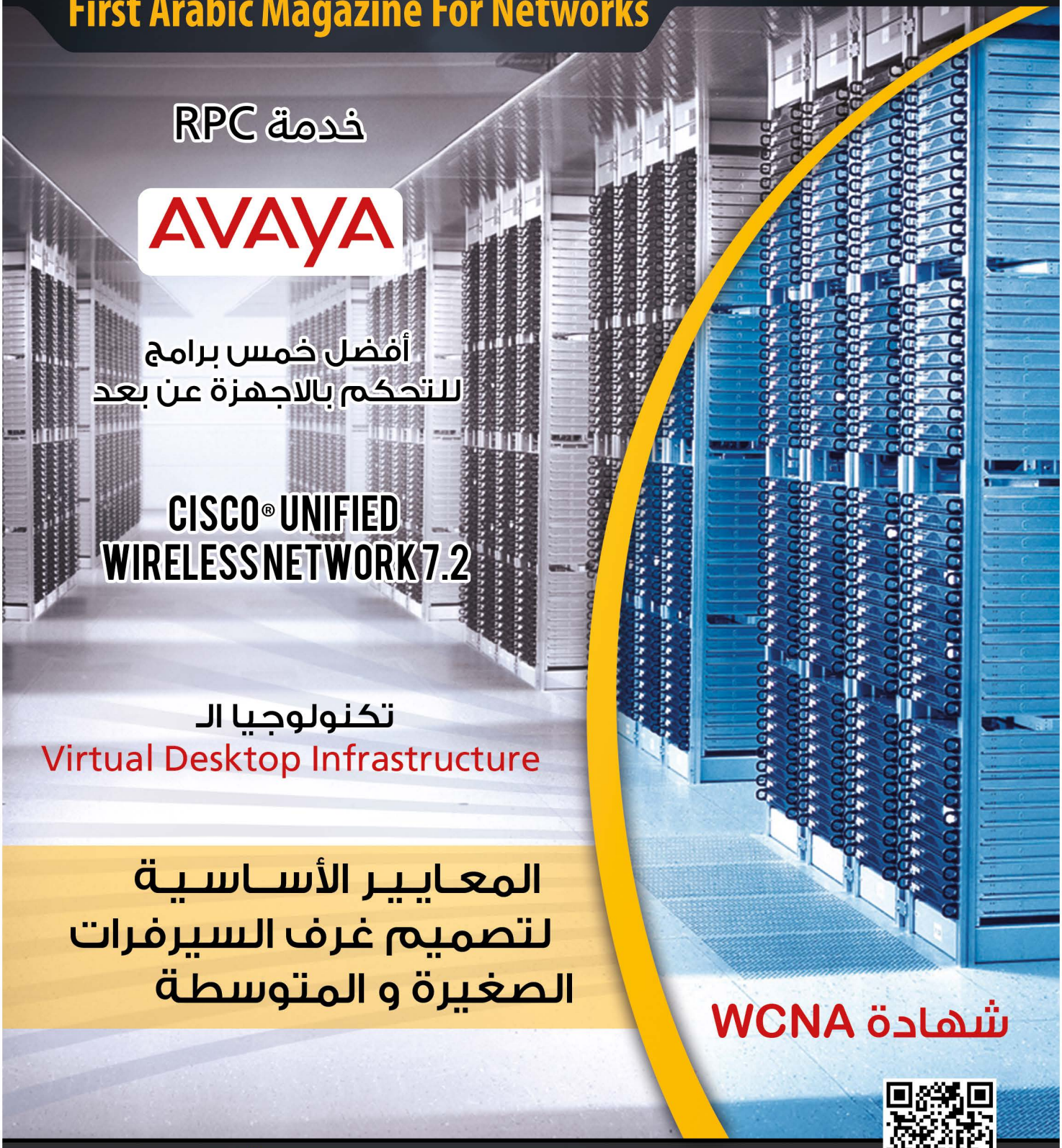
NO. 29 • September 2012 • Price Free • www.networkset.net

NetWork Set

First Arabic Magazine For Networks



خدمة RPC

AVAYA

أفضل خمس برامج
للتحكم بالاجهزة عن بعد

CISCO® UNIFIED
WIRELESS NETWORK 7.2

تكنولوجيا الـ
Virtual Desktop Infrastructure

المعايير الأساسية
لتصميم غرف السيرفرات
الصغيرة و المتوسطة

شهادة WCNA

www.networkset.net

العودة إلى الفهرس

الثغرة الكبيرة

عندما تصلني رسالة على البريد الخاص تعلمني بأن الشخص المرسل فقد الأمل في إيجاد فرصة عمل مناسبة وهو من الناحية الأكاديمية جاهز, خريج جامعي, حاصل على عدة شهادات احترافية أكثر من ,CCNA MCITP وطبعا بدون خبرة ميدانية في ساحات العمل, المشكلة أكيد تبدأ بالخبرة لكن أعتقد أن الجميع لازال يتوهم سمعة الـ IT كما كانت قبل ست أو سبع سنوات, وظيفة جيدة ومدخولها جيد, وهذا صحيح وغير صحيح.

في البداية أريد أن أخبركم بأن هناك ثغرة كبيرة في عالم الـ IT بشكل عام وهو ازدياد عدد المتعلمين عن العدد المطلوب وهذا يعود إلى سمعة المجال التي مازالت منتشرة حتى هذه اللحظة والتي أعتقد أنها انخفضت كثيرا عن السابق, فمروجي المعاهد التدريسية مازالوا يرسموا للطلاب ذلك الحلم الكبير والوظائف الكثيرة التي تنتظرهم من باب الدعاية والإعلان لكورساتهم وأنا بمقالي هذا لا اريد أن أقطع برزق أحد من المدرسين لكن اتمنى منهم أن يكونوا محقين في هذا الأمر وبأن لا يجعلوا البحر كالعسل فهذه أمانة ويجب أن يقدم الجميع الصورة المتوقعة لمجال العمل للطالب حتى لا تتحمل ذنبه يوم من الأيام. أما الطالب والمتخرج فيجب أن يكون عقله متفتح أكثر وأن يبتعد قليلا عن السير مع القطيع فلو أردت أن تحصل على شهادات فلا تكثر منها, أحرص على دراستها لكن لا تحاول اقتنائها كلها فمجال التكنلوجيا متسارع بشكل كبير ولو كنت ما زلت تعتقد ان سيسكو هي المسيطر فأنت مخطئ تماما في توقعاتك وأجزم والله اعلم أن الطلب على شهادة مثل الـ CCIE في العالم العربي سوف ينعدم قريبا, فالتنافس الآن كبير والكل يريد أن يأخذ حصته في عالم الـ IT إلا نحن نريد أن نستهلك هذا القطاع الذي تقدر بعض الإحصائيات قيمته بأكثر من 500 مليار دولار سنويا تذهب لهم ونحن نراوح في مكاننا.

الخطة التي سوف اقدمها لك جيدة وبسيطة وأنا طبعا غير مقتنع بها كثيرا لأن من الأشخاص الذي ينادي بالتميز في مجال لكن سوف أخبرك بهذه الخطة حتى تبتعد عن سيسكو قليلا. الـ CCNA, MCITP لابد منهم ولا تزد عليهم بشيء أكثر احترافية كالدخول في مجال الـ CCNP, زود نفسك بشهادة من جونيبر ولو كانت أبسط واحدة فيهم وزود نفسك بشهادة من VMWare ولو أمكنك الحصول على شهادة في الامن والحماية فهذا جيد أيضا.

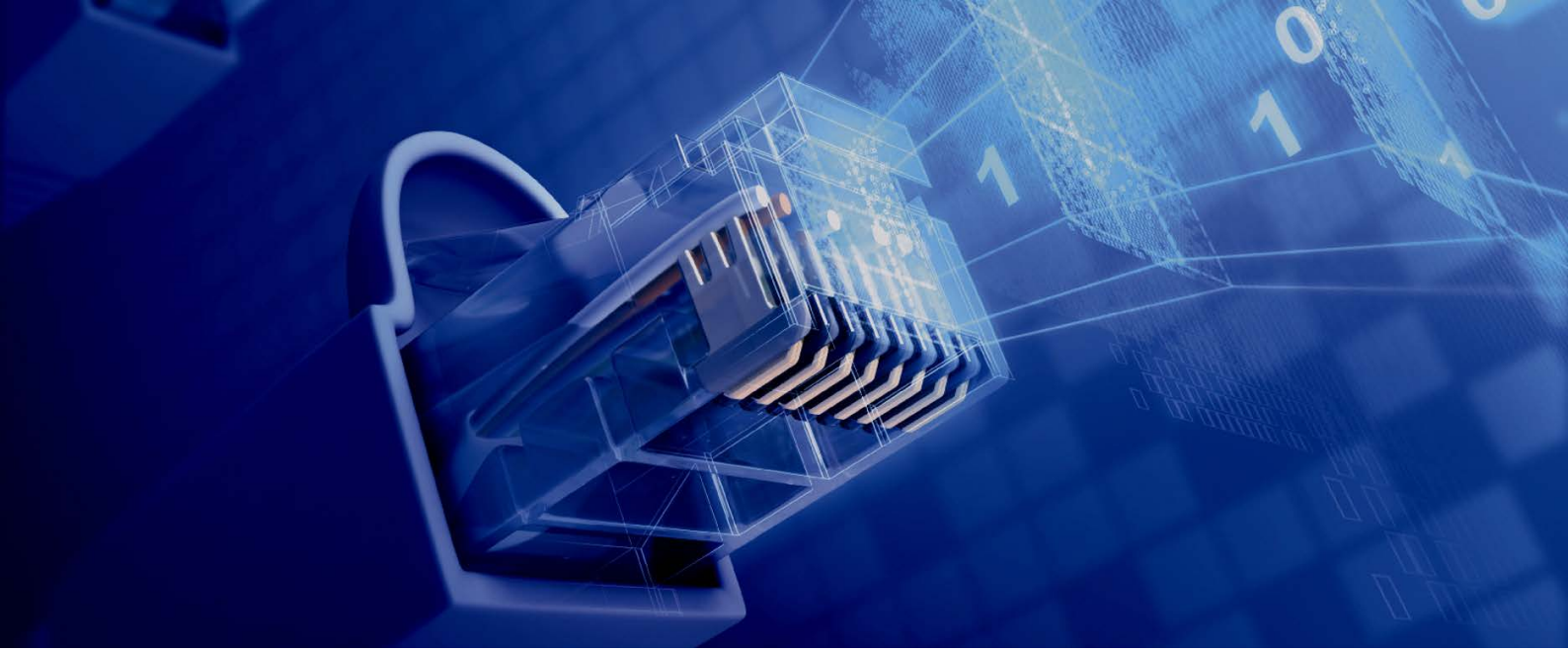
أحرص على التدريب والتعلم على أنظمة الفايروول التي أغلبها يسمح لك بتحميل نسخة Virtual وعلى قناتنا على اليوتيوب هناك سلسلة شروحات حاول الاستفادة منها. أحرص على تعلم برامج النسخ الاحتياطي ولكن لديك في سيرتك الذاتية إيجادة لأكثر من ثلاث برامج احترافية. تابع جديد عالم الشبكات والـ IT بشكل عام من خلال الاشتراك بالمواقع المتخصصة والتي تقدم معلومات جديدة في هذا المجال.

لو طبقت كل هذه الامور ولم يسعفك الحظ في وظيفة مناسبة فما هو الحل البديل ؟ الحل البديل الذي أقترحه عليك هو أن تبدأ عملك الخاص لكن أبحث عن التمييز فيه, حاول أن تركز كل جهودك في شيء جديد يتوقع له خيرا في المستقبل القريب, أستفد من المنتديات العربية والمواقع الأجنبية لمعرفة أكثر نوع من المشاكل يمر به الناس في عملهم وأجلس على غوغل طويلا باحثا عن أفضل الحلول وأجعلها جزء من شركتك أو عملك الخاص, خذ على سبيل المثال مشكلة بطئ الـ VPN بين الشركات التي تشارك قواعد بياناتها مع فروع أخرى الآلاف يعانوا من هذه المشكلة, النسخ الاحتياطي للملفات والتي عادة ما تكون مشاكلها كارثية, تعلم كيفية استخراج الداتا من الهاردات التي تتوقف عن العمل لأسباب فنية, هناك كورسات وأدوات متخصصة في هذا المجال. العالم مفتوح أمامك لكن لازال الكثيرين منكم ينتظر الإرشاد والتوجيه وغير راغب برفع معدل استخدام عقله لثلاثة بالمئة.

خلاصة هذا الكلام هو التميز ليس في الأختصاص فقط بل التميز في التفكير التميز في نظرتك لعالم العمل, أغلق هذه الفجوة الهائلة بين المتقدمين للعمل والمطلوبين للعمل من خلال فتح مجالات جديدة أمام الشركات, فكرة واحدة كافية لتضعك في سوق العمل لكن أعطها حقها من الوقت والبحث وكون أنت الاول والمبادر ودمتم بود.

أيمن النعيمي - سوريا

العودة إلى الفهرس



مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

أسـرة المجلـة

المؤسس و رئيس التحرير

م.أيمن النعيمي

المحـررون

م.نادر المنسي	عباس موسى عودة	فادي أحمد الطه
م. عادل الشبل	محمد أحمد يوسف	---
م. أحمد هيكل	حسام الدين حشيش	---
أحمد خير الدين	خالد الدسوقي	---

التصميـم و الاخـراج الـفني : محـمـد زرقـة

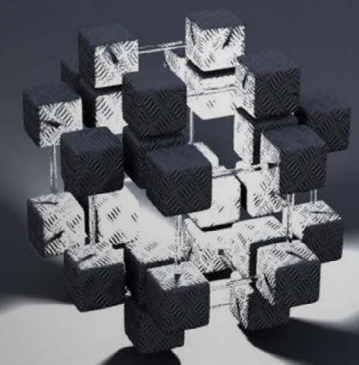
مدقق أملائي ونحوي للمجلة : أسـامة كـامـل

www.networkset.net

تقرؤون في هذا العدد

NetWork Set

First Arabic Magazine For Networks



ICMP Redirect

يعتبر هجوم الـ ICMP Redirect أحد الهجمات الخطيرة والغير معروفة كثيرًا في الأوساط التقنية لذلك قررْت أن يكون مقالي الأول في مجلة NetworkSet يدور حول هذا الهجوم وآلية عمله وكيفية تنفيذ هذا النوع من الهجمات، بداية سنلقي نظرة سريعة على بروتوكول ICMP ،فهذا البروتوكول كما يعرف عنه يستخدم لاختبار الاتصال والتعرف على مشاكل الاتصال بين جهازين على مستوى الطبقة الثالثة layer 3 فهو يعرّف على أنه Messaging Protocol أو Reporting Protocol حيث أن مهمته هي إرسال تقرير حول المشكلة فى الاتصال أو الوصول للطرف الآخر وسبب هذه المشكلة بالتّالي يختص فقط بإرسال معلومات حول حالة الاتصال ووجود مشكلة ما وليس لإصلاح هذه المشكلة.

ولهذا البروتوكول العديد من أنواع الرسائل والتى تستخدم كل منها فى غرض معين أو فى حالة معينة فمثلا:

Echo Request (Type 8)

هذة الرسالة من أشهر استخدامات الـ ICMP والتي تستخدم مع أمر ping لاختبار وجود الطرف الآخر من الاتصال.

Echo Reply (Type 0)

فى حال إن كان الطرف الآخر حيًا فيرد على الـ Echo request بهذه الرسالة.

Destination Unreachable (Type 3)

وهذه الرسالة تعني أنه تعذّر الوصول للطرف الآخر ونلاحظ أن رسائل الـ ICMP لها ما يعرف بال code وهو رقم من خلاله يتم التعرف على سبب المشكلة فمثلا Type 3 code 0 يخبرنا بأنه لا يمكن الوصول للطرف الاخر لأنه لا يمكن الوصول لهذه الشبكة، أما Type 3 code 13 فهذا يعنى أنه لم يتم الوصول للطرف الآخر لأنه تم منع الاتصال من قبل جهة ما، وطبعًا هنا يشار إلى الجدار الناري.

Type 11 Time Exceeded Message

ترسل هذه الرسالة إلى المرسل لإخباره أن الـ packet قد انتهت لأن قيمة الـTTL قد وصلت الى الصفر.

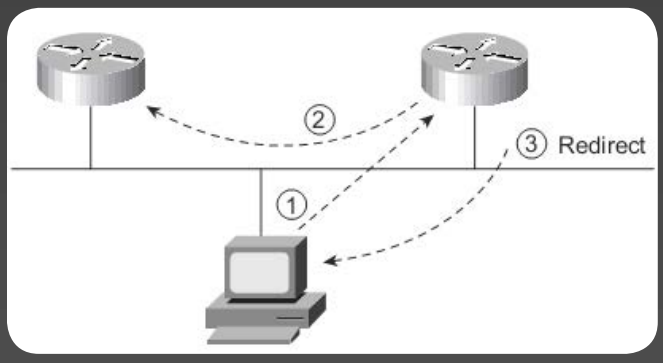
Source quench message (Type 4)

ترسل هذه الرسالة من أحد الطرفين للآخر لتقليل معدل إرسال البيانات وذلك بسبب مشاكل الزحام أثناء نقل البيانات.

ICMP Redirect (Type 5)

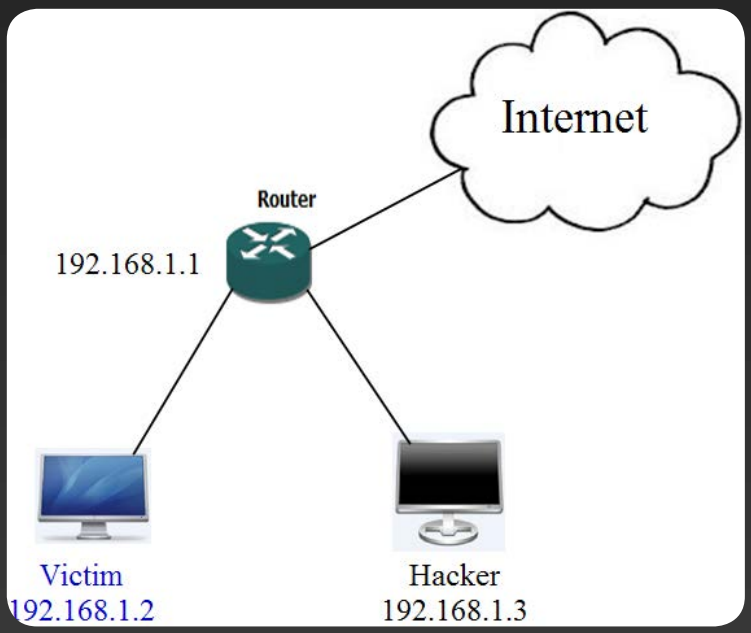
وهذا النوع هو موضوعنا اليوم، لنرى كيف يستخدم هذا النوع من الرسائل وكيف يتم استغلاله من قبل الهاكرز لسرقة البيانات.

لو فرضنا أنه لدينا شبكة متصلة بأكثر من راوتر أي أن لها أكثر من default gateway ولكن أجهزة هذه الشبكة معدة لاستخدام أحد هذه الراوترات فقط كالـ default gateway فإذا أراد أحد المستخدمين الوصول لشبكة معينة



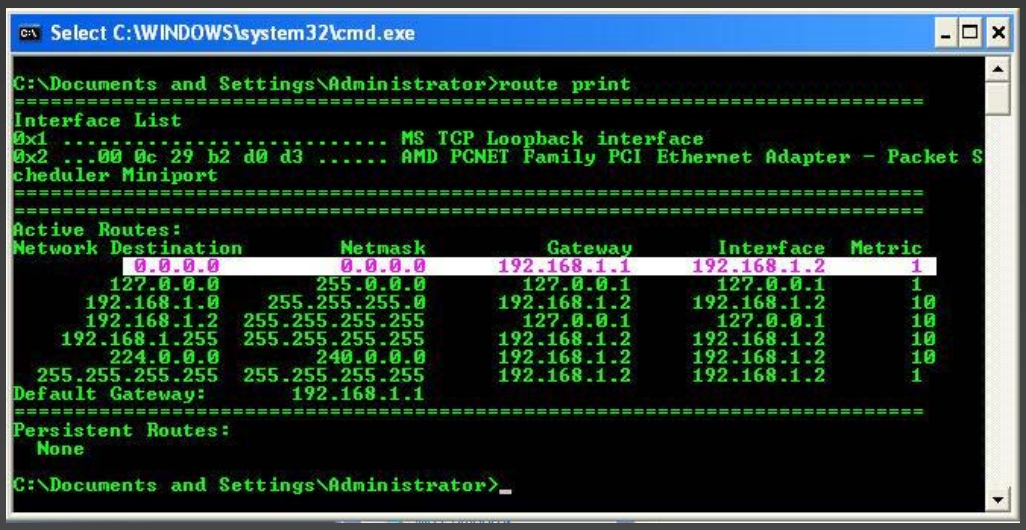
ورأى هذا الروتر وهو الـ default gateway أن أفضل وصول للمستخدم لهذة الشبكة هو من خلال الراوتر الآخر وليس من خلاله، وبالتالي يرسل للمستخدم رسالة ICMP Redirect يخبره فيها أنه للوصول لهذه الشبكة عليك الذهاب إلى الراوتر الآخر واستخدامه كالـ default gateway.

هنا استغل الهاكرز هذا النوع من الرسائل بإرسال رسالة من هذا النوع للضحية ليقنع جهاز الضحية باستخدام جهاز الهاكر كـ Default gateway للوصول إلى شبكة معينة أو عنوان معين، وهكذا استطاع الهاكر الحصول على نسخة كاملة من البيانات التى يرسلها جهاز الضحية قد يقوم بتحليلها والاستفادة من محتواها فى سرقة بيانات الضحية سواء كلمات مرور أو غيرها



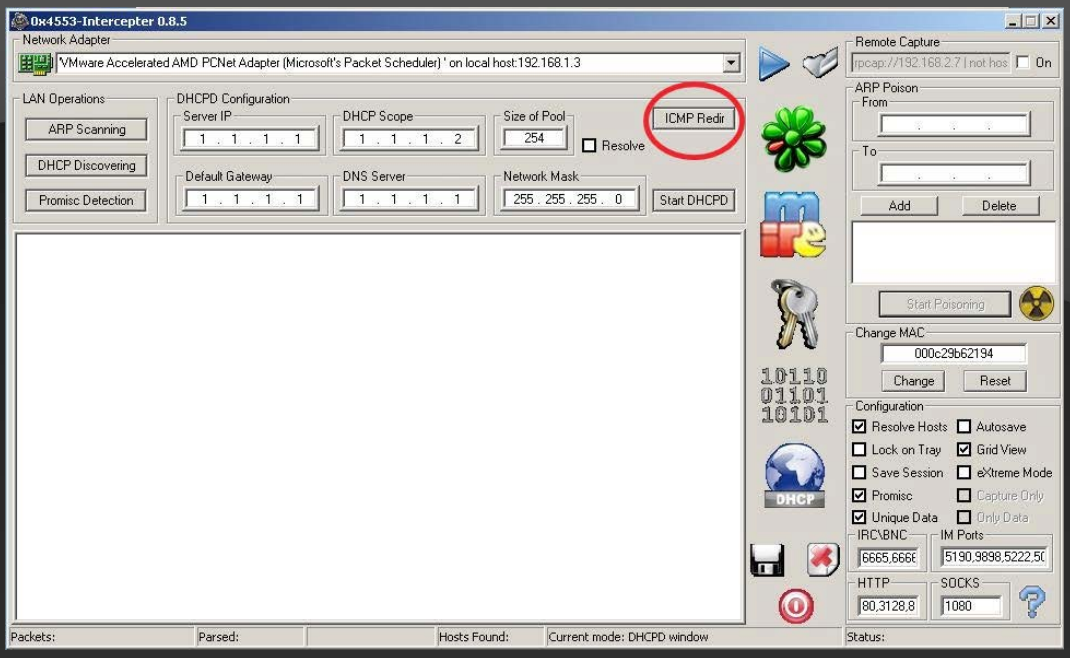
نأتي للتنفيذ العملي ونقوم بتنفيذ هذا السيناريو كما هو موضح بالشكل، جهاز الهاكر عنوانه 192.168.1.3 وجهاز الضحية192.168.1.2 والـ default gateway لهذة الشبكة هو 192.168.1.1

قبل أن نبدأ، سنذهب إلى جهاز الضحية ونتأكد أن أي ترافيك يتم إرساله خارج الشبكة يرسل إلى الـ default gateway وهو192.168.1.1 بالأمر route print.



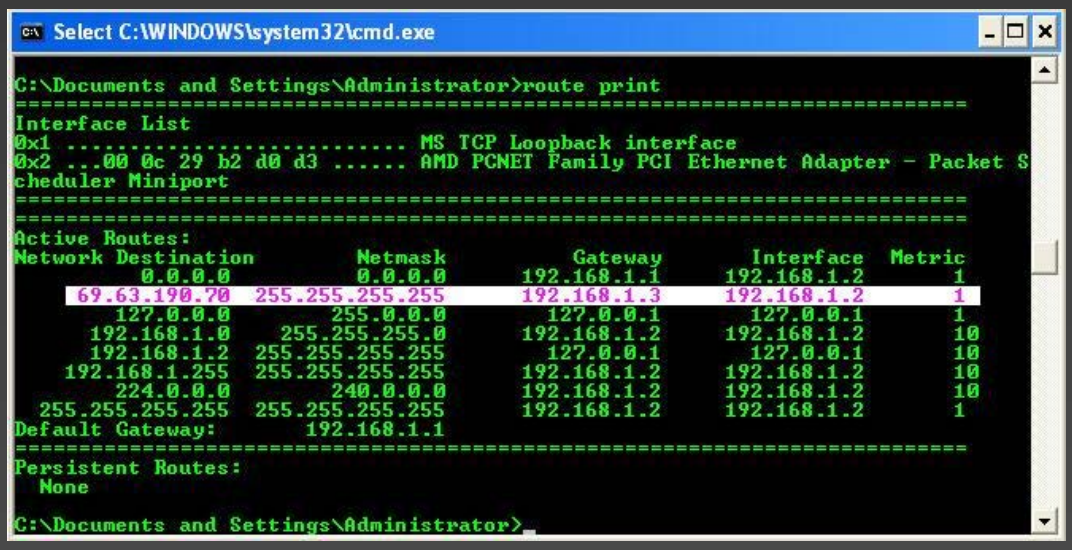
سيقوم الهاكر بإرسال ICMP Redirect لجهاز الضحية وذلك ليجبره على إرسال الترافيك المرسل إلى عنوان معين وليكن عنوان موقع الفيس بوك مثلا إلى جهاز الهاكر ليصبح جهاز الهاكر هو الـdefault gateway للوصول لهذا العنوان، ولذلك يقوم الهاكر أولا بالحصول على ip موقع الفيس بوك بالأمر ping www.facebook.com وهو 69.63.190.70 .

ثم نذهب إلى أداة 0x4553-Intercepter ثم بالضغط على زر DHCP ثم ICMP Redir

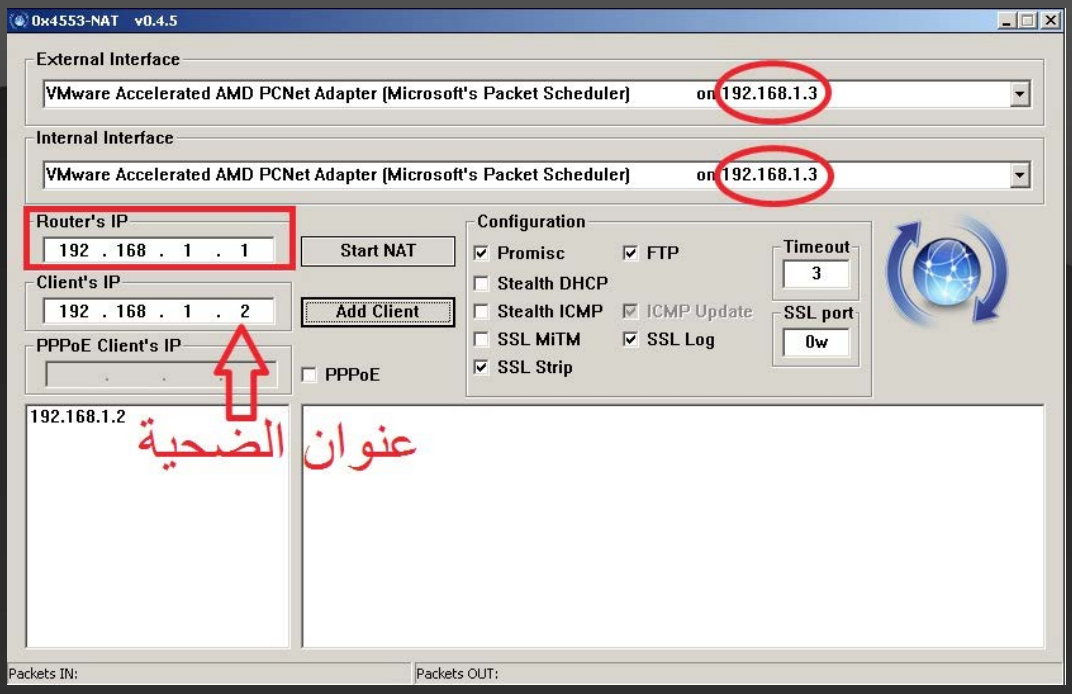


ونضيف العناوين كما هو موضح بالصورة ثم نضغط Send Packet.

للتأكد من عمل البرنامج وأن الترافك الذي سيرسله جهاز الضحية للعنوان المذكور سيمر عبر جهاز الهاكر، نعيد عليه أمر route print ونلاحظ ظهور route خاصة بهذا العنوان مستخدمة جهاز الهاكر كـ default gateway.



ونأتي لجزء مهم، وهو: أنه يجب أن يقوم الهاكرز هذا الترافك إلى الإنترنت حتى لا يشعر الضحية بأن شيئا ما خطأ يحدث وهنا سنستخدم عملية الـ NAT لإعادة توجية الترافك.
فى نفس مجلد البرنامج نفتح الأداة 0x4553-NAT ونضع العناوين كما هو موضح بالصورة.
ثم نضغط Add Client ثم Start NAT.



هذا الهجوم يسمى (Man In The Middle (MITM وقد نفذناه بخاصية الـ ICMP Redirect.
يبقى على الهاكر تحليل هذا الترافك المار من خلاله والحصول على المعلومات الموجوده به وهذا سنتحدث عنه فى مقالات قادمة بإذن الله تعالى.

الإجراءات الوقائية من هذا الهجوم Countermeasures:

أولاً: إيقاف خاصية الـ ICMP Redirect لنمنع الكمبيوتر من الاستجابة لهذا النوع من الرسائل وذلك بالتعديل فى الريجيسترى بالأمر regedit ثم نذهب إلى المسار:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

ثم نفتح EnableICMPRedirect ونغير قيمتها من 1 الى صفر.

ثانياً: الاستعانة ببرامج الحماية القوية لصد مثل هذا الهجوم مع تحديثها الدائم ومن أشهر هذة البرامج Eset smart security 5.

الأداة المستخدمة فى الشرح يمكن الحصول عليها من هذا الرابط.
http://sniff.su/0x4553-Intercepter.v085.zip

NetWork Set

معنى جديد لعالم الشبكات
في سماء اللغة العربية

الموسوعة

Wiki.NetworkSet

أول موسوعة عربية حرة
و متخصصة في مجال الشبكات

GO زيارة الصفحة

المجلة

أول مجلة عربية متخصصة
في مجال الشبكات

GO زيارة الصفحة

المدونة

NetworkSet

مدونة عربية متخصصة
في مجال الشبكات

GO زيارة الصفحة

(س) و (ج)

قسم خاص
بالأسئلة والاجوبة

GO زيارة الصفحة

القناة

YouTube

قناة المدونة
على موقع يو تيوب

GO زيارة الصفحة

ترجم

أول مشروع عربي لترجمة
المواد العلمية و التقنية

GO زيارة الصفحة

Email: networkset@Bhotmail.com | www.networkset.net

How to write a Script II
(If Statement)

تعرفنا فى المقال السّابق على بعض الأوامر التى تساعدنا فى القيام بكتابة اسكريبت بشكل احترافي.
والآن أيضًا سنقوم بالتحدّث فى بعض الأدوات التى تساعدنا هى الأخرى على القيام بذلك وهى If Statement .

فى البداية يجب علينا أن نقول أنّ If Statement هى حالة شرطية، بمعنى أنها تقوم بعمل Check على شىء معين وإذا تحقق هذا الشىء فإنها تنفذ أمر أو أوامر معينة أما إذا لم يتحقق فإنها تقوم بتنفيذ أمر أو أوامر أخرى تقوم انت بتحديدها فى Syntax الذى تكتب به if Statement .

ملحوظة: عمليةcheck التى تقوم بها if statement تكون فى الأغلب من خلال test command المذكور فى المقال السابق.

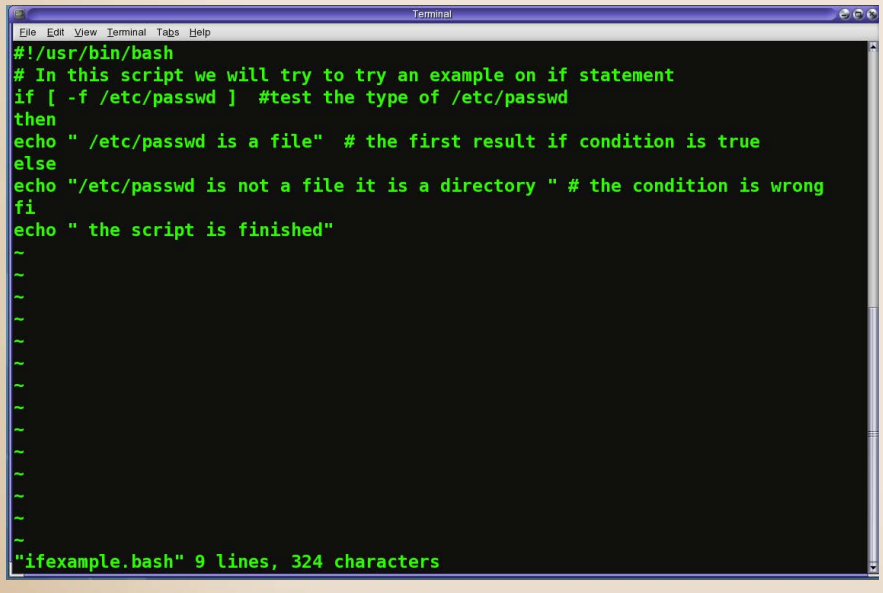
الآن تعالوا بنا لنتعرف على كيفية كتابة if statement :

```
$ if command1
> then
> execute command2
> else
> execute command3
> fi
```

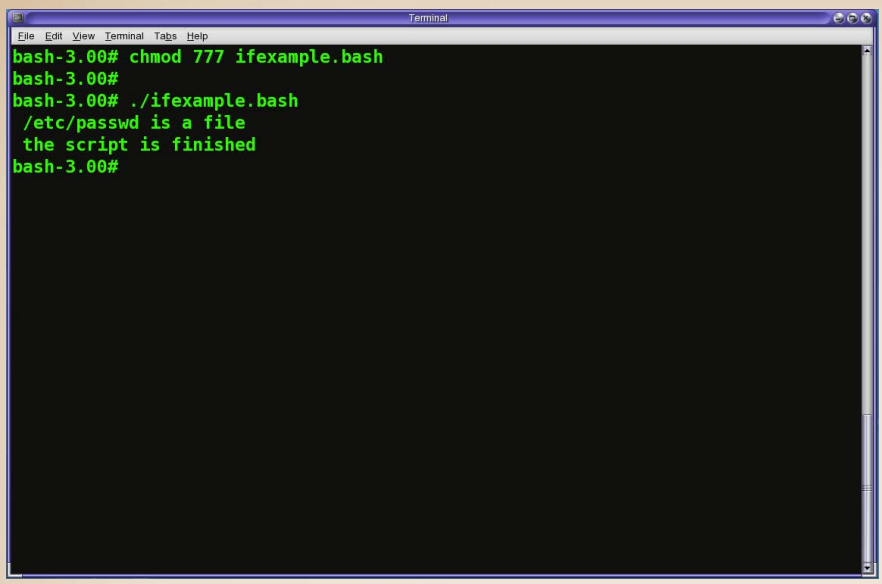
- Command 1 فى الغالب يكون من خلال test command.
- Command 2 الأمر أو الأوامر التي تنفذ فى حالة ما كان test command صحيح أي انه $?echo خرجها صفر.
- Command 3 الأمر أو الأوامر التي تنفذ إذا كان test command خرجها ليس صحيح أي انه $?echo أي قيمة غير الصفر.

مثال 1:

دعنا نكتب سكريبت يعمل check ما إذا كان /etc/passwd عبارة عن ملف



ولتنفيذ هذا الاسكريبت يجب علينا أن نحفظه ثم نعطيه permission حتى نستطيع تشغليها وستكون النتيجه كالتالي:



While command

while هى أيضاً أحد الأدوات التى نستخدمها لكى نقوم بعمل check على شىء ما فى النظام الذي نعمل عليه ولكنها تختلف عن if statement فى أنها عبارة عن loop بمعنى أنه طالما condition موجود وصحيح فإنه loop تستمر فى عملها حتى يصبح هذا الشرط غير صحيح وبالتالي تتوقف عن العمل.

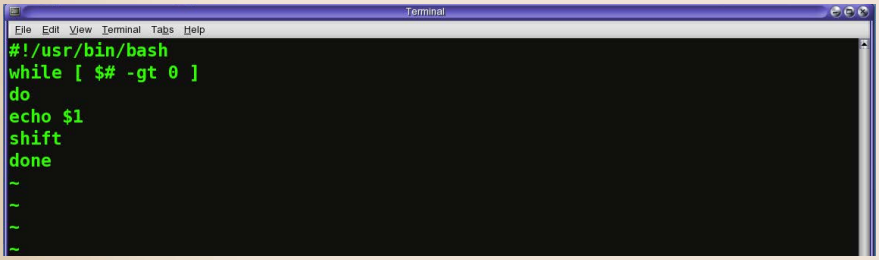
كيفيه كتابه while statement :

```
$ while command1
> do
> command2
> done
```

- Command 1 وهو الشّرط الموجود والذي طالما يكون صحيح فإنloop تستمر في العمل.
- Command 2 الأمر أو مجموعة الأوامر التى تنفذ طالما الشرط صحيح.
- Done معناها إذا أصبح الشّرط غير صحيح فإنك تخرج من loop كلها.

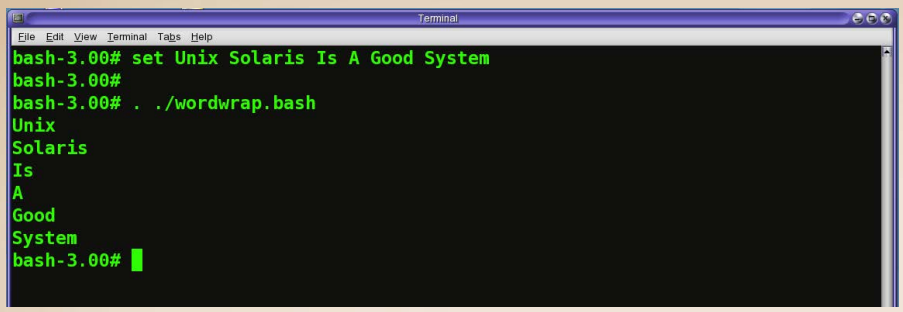
مثال 2:

فلنقل مثلاً أننا نريد إعادة كتابة جملة كل كلمة فى سطر بدلاً من أن تكون جميع الكلمات بجانب بعضها البعض:



شكل لتوضيح الاسكريبت

بعد ذلك نقوم بتغير permission على الملف ثم نقوم بتشغيله فتكون النتيجة كالتالي:



الآن...

سنقوم بالتعرف على خاصّية مهمة جدًا فى كتابة الشل، وهي كيفية جعل الأمر لاينفذ إلا بوجود أمر معين أو حدث معيّن قبله، لماذا؟

نحتاج إلى هذا فى بعض الاحيان. نحتاج فى الاسكريبتات الى تشغيل service معينه وليكن مثلا NFS ولكي تعمل على النظام لابد من وجود service أخرى موجوده على النظام،وهنا يظهر الاحتياج إلى جمع الاثنين مع بعضهما فلا تعمل NFS Service إلا إذا كانت جميع services التى تعتمد عليها موجودة وتعمل على النظام.

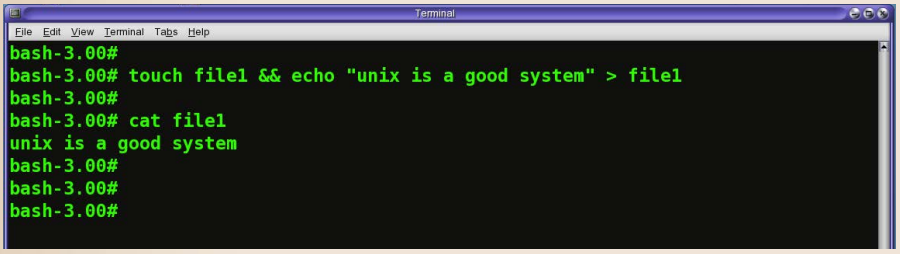
دعنا نقوم بضرب مثال للتوضيح لنعرف كيفية كتابة syntax الخاص بها.

مثال 1:

سنقوم بإنشاء ملف معين ثم نقوم بالكتابة فى داخله، هنا لا نستطيع الكتابة بداخل الملف إلا اذا كان الملف موجود.

Touch file1 && echo «Unix is a good system» > file1

عند القيام بهذا وقراءة الملف file1 تكون النتيجة كالتالي:



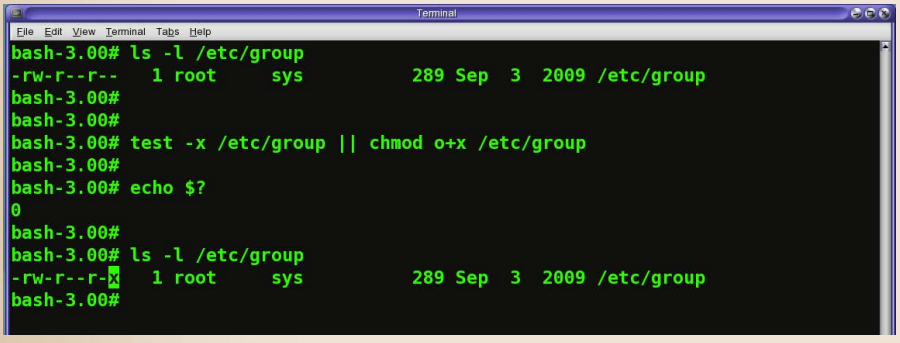
فى هذه الحالة && تعني أنه لا تنفّذ الأمر الثاني إلا إذا كان الأمر الأول نفذ وبشكل صحيح أيضًا.

مثال 2:

نحن نريد أن نعطى ملف معين x» execute permission» فى حالة إذا كان ليس موجود على الملف لعمل ذلك نقوم بالآتي:

Test -x /etc/group || Chmod o+r /etc/group

لعمل ذلك نقوم بما هو موضح فى الشكل.



فى هذا المثال علامة || تتأكد أنه الأمر الأول لم يتم تنفيذه بشكل صحيح لذلك قام بتنفيذ الأمر التالي.

Case Statement

Case مثلها مثل if هي أيضاً حالة شرطية ولكنها هنا تقبل العديد من الحالات فمثلا if تفرق بين شيئين أما condition صحيحة فتنفذ أمر معين وأما خطياً فتنفذ أمر آخر أما هنا فإن case statement تقبل العديد من conditions.

Case syntax

```
Case value in

  Cond.1)
            Command 1
            Command 2
    ;;
  Cond.2)
            Command1
            command2
    ;;
  |
  |
  |
    ;;
    *)
          Command 1
          Command2
;;
esac
```

والآن أترككم مع مثال عملي كواجب لكم يدل على مدى الاستعياب من المقالات نحن نريد أن نقوم بعمل سكريبت يضيف المستخدمين إلى النظام بشرط أن لا يكونوا موجودين قبل ذلك على النظام فإذا كان المستخدم موجود فإنه يظهر رسالة error : user is existed on the system.

وإلى اللّقاء فى مقالات أخرى إن شاء اللّه.

OSPF LSA Types

مقال هذا العدد سوف يكون شرح أنواع الـ Updates في الـ OSPF التي يغطّيها منهاج الـ CCNP .

طريقة الشّروحات التي سوف اعتمدها في أغلب مقالاتي تعتمد على جزئين: النظري والعملي، لقناعتي أنّ كلاهما سوف يكون مُكمّل للآخر، بمعنى إنْ كان هناك نوع من الغموض في القسم النظري سوف يوضحه العملي و العكس صحيح، باستثناء التّفاصيل الواردة و بكثرة في محركات البحث ومن السهل الوصول إليها، سوف أتناولها مروراً فقط ويكون التركيز على التّفاصيل الغير الواردة أو التي يلفها الغموض وذلك لتجنب التّكرار، كما أنه من الممكن ملاحظة نوع من التّكرار في التّراكيب و الجمل أثناء الشّرح وهو متعمَّد لتعميق الفهم، لذا اقتضى التنويه.

القسم النظري

أنواع الـ LSA:

A. (LSAtype 1 (Router LSA: تتبادل جميع الرّاوترات المشتركة في نفس الـ Area هذا النوع من الـ Update ، بمعنى آخر هذا النوع يكون فقط في نفس الـ Area.

B. (LSAtype 2 (Network LSA: يستخدم هذا النّوع من قِبل الـ DR (Designated Router) الذي يخبر باقي الرّاوترات بالتّغيرات التي تطرأ على الشّبكة و الرّاوترات الموجودة، وكذلك إنّ هذا النّوع يكون فقط في نفس الـ Area.

C. LSAtype 3 (Summary Network LSA): أما هذا النّوع يستخدم من قِبل الـ ABR و الذي يخبر من خلالها عن جميع الرّاوترات التي تعمل باستخدام الـ OSPF الموجودة خارج الـ Area بمعنى آخر عند انتقال الـ Update من Area إلى أخرى يكون ذلك باستخدام هذا النّوع.

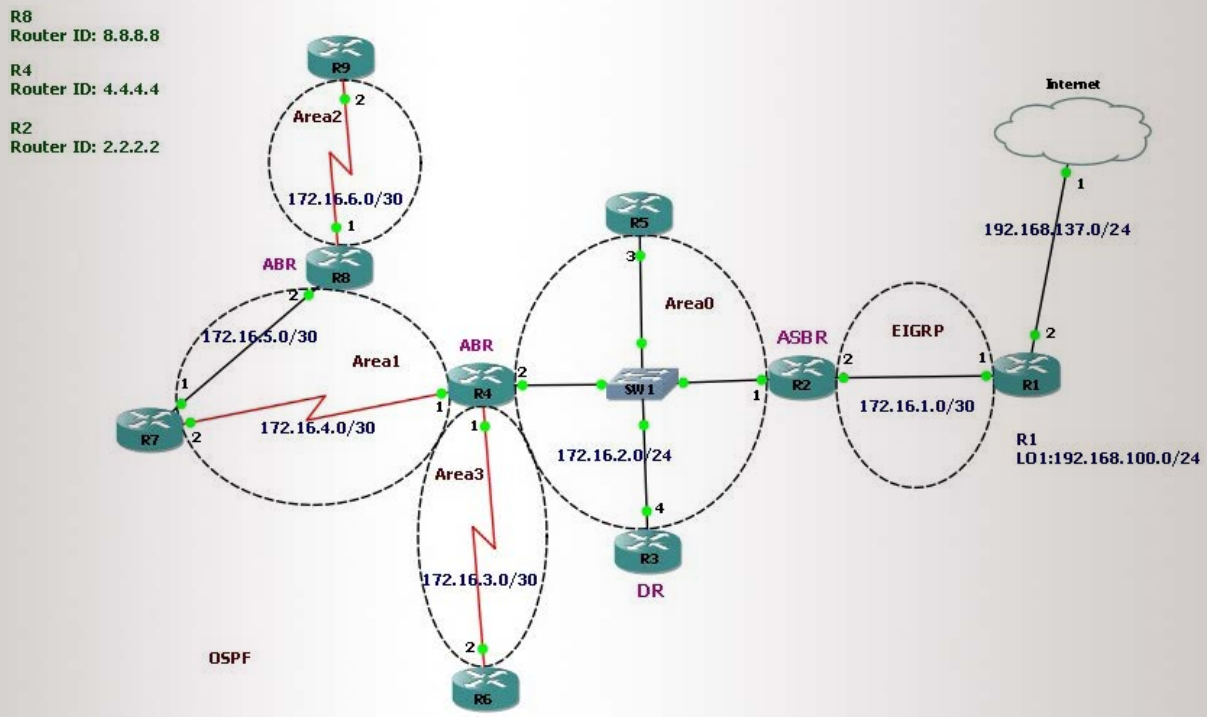
D. (LSA type 4 (Summary ASBR LSA:
في الواقع إنّ هذا النّوع هو الذي دفعني لكتابة المقال برمته لكثرة الأخطاء الواردة في محركات البحث أثناء توضيحه، هنا يجب الإنتباه إلى أن هذا النوع يستخدم من قبل الـ ABR للإعلان عن الـ ASBR وبالتالي الوصول إلى الشّبكات الخارجيّة المطلوبة بالوقت ذاته، أعلم أنه لايزال هناك بعض الغموض الذي سوف يوضّح في القسم العملي بعون اللّه.

E. (LSA type 5 (External LSA: لنقُل أنّ هذا النّوع يعمل على الرّاوتر الذي يمثّل الـ Gateway بالنّسبة للـ OSPF Network ، لذا أقول نعم، هذا هو النّوع الذي يستخدم من قبل الـ ASBR (Autonomous System Boundary Router) و الذي يستخدم للإعلان عن جميع الشّبكات الخارجيّة المتّصلة به ببروتوكولات مختلفة وكذلك الـDefault Route و إذاعتها ضمن الـ OSPF Network.

WHAT IS OSPF LSA

القسم العملي

هنا سوف نقوم بإنشاء LAB لتوضيح ما سلف، وهو عبارة عن OSPF Network بالإعتماد على أجهزة سيسكو:



لنفترض وجود السيناريو الذي يقول أنه تم إضافة شبكة جديدة إلى R1 و التي سوف نمثلها على شكل Loopback وهي 24/192.168.100.0 ، والسؤال هنا كيف سوف ينتقل الـUpdate في الشبكة ؟ : بعد انتقال الـ Update من خلال الـ EIGRP من R1 الى R2 ، يأتي هنا دور الـ OSPF على الشكل التالي:

LSA TYPE 5

إنّ هذا النّوع يستخدم من قبل R2 في الإعلان عن جميع الشّبكات الخارجية التي أعلن عنها باستخدام EIGRP و الـ default route فهو يعلن عن كل من:
192.168.100.0/24 - 0.0.0.0 - 172.16.1.0/30 - 192.168.137.0/24

LSA TYPE 1

كما ذكرنا أن هذا النّوع يظهر جلياً وهو للتخاطب بين الرّاوترات الموجودة في نفس الـ Area0 كما في R2

بالذّهاب الى R2 و إظهار أنواع الـLSA التي ينشِئُها يتبين لنا التالي:

```
R2#show ip ospf database self-originate

            OSPF Router with ID (2.2.2.2) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
2.2.2.2         2.2.2.2         644         0x80000008 0x001384 1

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         2.2.2.2         644         0x80000002 0x00FCAC 1
172.16.1.0      2.2.2.2         644         0x80000002 0x0007D5 0
192.168.100.0   2.2.2.2         644         0x80000002 0x00A722 0
192.168.137.0   2.2.2.2         644         0x80000002 0x000F95 0
R2#
```

نستطيع أن نلاحظ هنا أنه قام بإنشاء نوعين من الـ LSA هما النّوع LAS1 و LSA5، أما النّوع الأول فهو للإعلان عن نفسه في الـ Area0 و النّوع الخامس للإعلان عن الشّبكات الخارجية المتصلة به وعن الـ Default route .

LSA TYPE 2

يقوم R3 بإنشاء هذا النّوع على اعتباره هو الـ DR و مخاطبة جميع الراوترات الموجودة في الـ Area0 باستخدام هذا النوع لإخبارهم بالتّغيّرات التي تطرأ على الشبكة.

بالذهاب الى R3 و إظهار أنواع الـLSA التي ينشِئها يتبين لنا التّالي:

```
R3#show ip ospf database self-originate

            OSPF Router with ID (172.16.2.4) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.2.4      172.16.2.4      197         0x80000008 0x0053CD 1

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.2.4      172.16.2.4      197         0x80000003 0x008E7F
R3#
```

إذن، على اعتبار أنَّ الـDR يقوم بإنشاء LSA1 and LSA2 وفي حال أنه لم يكن الـ DR سوف يقوم بإنشاء LSA1 فقَط كما في R5.

```
R5#show ip ospf database self-originate

            OSPF Router with ID (172.16.2.3) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.2.3      172.16.2.3      1345        0x80000004 0x005DCA 1
R5#
```

LSA TYPE 3, 4

النوع الثالث يقوم بإنشاؤه كل من R4 وR8 على اعتبارهم الـ ABR و يكون ذلك للإعلان عن الرّاوترات المتّصلة بهم في الـAreas الأخرى، و النوع الرّابع للإعلان عن الـ ASBR.

بالذّهاب الى R4 وR8 وإظهار أنواع الـLSA التي ينشئها يتبين لنا التّالي:

```
Link ID         ADV Router      Age         Seq#       Checksum Link count
4.4.4.4         4.4.4.4         514         0x8000000D 0x00C18C 2

                Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.3.0      4.4.4.4         759         0x80000006 0x00D05A
172.16.4.0      4.4.4.4         514         0x80000006 0x00C564
172.16.5.0      4.4.4.4         514         0x80000006 0x00C463

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
4.4.4.4         4.4.4.4         514         0x8000000B 0x00072C 2

                Summary Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.2.0      4.4.4.4         759         0x80000006 0x0075F2
172.16.3.0      4.4.4.4         771         0x80000006 0x00D05A

                Summary ASB Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
2.2.2.2         4.4.4.4         772         0x80000005 0x00A876

                Router Link States (Area 3)

Link ID         ADV Router      Age         Seq#       Checksum Link count
4.4.4.4         4.4.4.4         773         0x80000008 0x00D666 2

                Summary Net Link States (Area 3)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.2.0      4.4.4.4         773         0x80000006 0x0075F2
172.16.4.0      4.4.4.4         564         0x80000006 0x00C564
172.16.5.0      4.4.4.4         564         0x80000006 0x00C463
172.16.6.0      4.4.4.4         565         0x80000006 0x003CAA

                Summary ASB Link States (Area 3)

Link ID         ADV Router      Age         Seq#       Checksum
2.2.2.2         4.4.4.4         809         0x80000005 0x00A876
R4#
```

كما نلاحظ أنه أعلن عن الـ ASBR باستخدام LSA4 و عن الرّاوترات في باقي الـ Areas باستخدام LSA3.

```
Link ID         ADV Router      Age         Seq#       Checksum Link count
8.8.8.8         8.8.8.8         1485        0x80000007 0x0035A0 1

                Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.4.0      8.8.8.8         1485        0x80000006 0x0057C1
172.16.5.0      8.8.8.8         1485        0x80000006 0x00C98E
172.16.6.0      8.8.8.8         1485        0x80000006 0x0037E0

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
8.8.8.8         8.8.8.8         1485        0x80000009 0x0082DC 1

                Summary Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.6.0      8.8.8.8         1485        0x80000006 0x0037E0

                Summary ASB Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
2.2.2.2         8.8.8.8         1516        0x80000005 0x00BC11

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
8.8.8.8         8.8.8.8         1517        0x80000009 0x0025ED 2

                Summary Net Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.2.0      8.8.8.8         1519        0x80000006 0x00898D
172.16.3.0      8.8.8.8         1519        0x80000006 0x00E4F4
172.16.4.0      8.8.8.8         1520        0x80000006 0x0057C1
172.16.5.0      8.8.8.8         1520        0x80000006 0x00C98E

                Summary ASB Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum
2.2.2.2         8.8.8.8         1520        0x80000005 0x00BC11
R8#
```

على هامش موضوعنا أود الإشارة إلى أنّ القاعدة في شبكات الـ OSPF تقول أنه على جميع الـ Areas الإتصال بالـBackbone Area ولكن كما في مثالنا هناك Area2 غير متصلة بـ Area0 و بالتّالي لن يكون هناك أي اتصال معها!
يكون الحل بعمل Virtual Link بين الـ ABR المشترك معه في الـArea وهو R8 و الـ ABR للـ Backbone وهو R4، يكون ذلك على الشكل التالي :

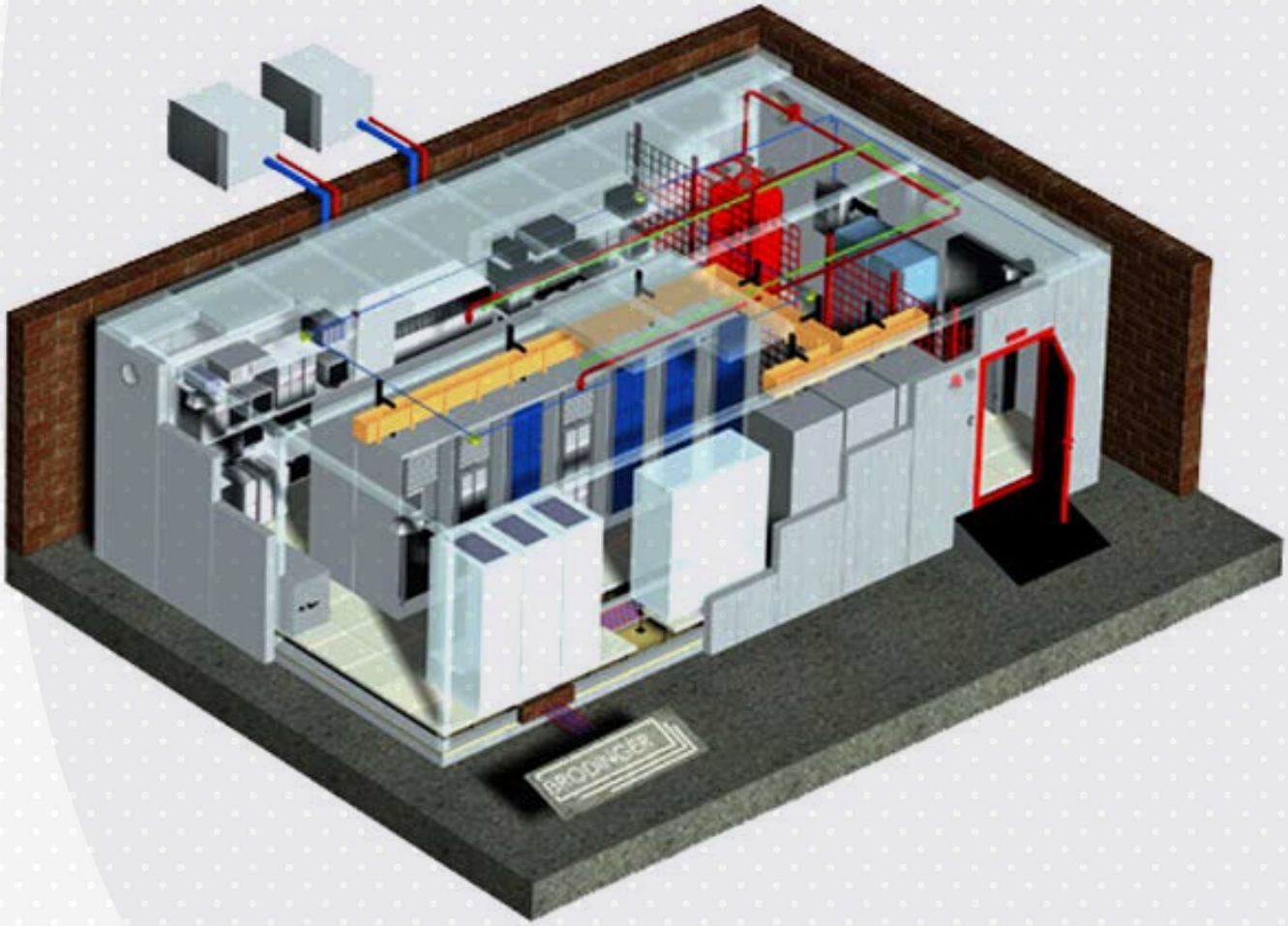
```
R8(config-router)#
R8(config-router)#area 1 virtual-link 4.4.4.4
```

```
R4(config-router)#
R4(config-router)#area 1 virtual-link 8.8.8.8
```

المعايير الأساسية لتصميم غرف السيرفرات الصغيرة والمتوسطة

لبناء أو تصميم غرفة سيرفرات كاملة والحصول على أعلى آداء ممكن في ظروف العمل المختلفة يتوجب على اي مصمم مختص العودة إلى معايير قياسية عالمية وضعتها جامعة كاليفورنيا والتى سوف نتعرف عليها في هذا المقال الأول من نوعه.

تعتبر هذه المعايير الضمان الوحيد الذي يكفل لك عمل السيرفرات خلال ظروف العمل الحرجة والعمل العادي على حد سواء. وكذلك في حال انقطاع التيار الكهربائي والحرائق والفيضانات، وحالات الطوارئ الأخرى.



General Space Characteristics

ROOM SPECIFICATIONS

مواصفات الغرفة:

1. المساحة تعتمد على عدد الأجهزة المطلوبة وحجم الشبكة حيث توفر مساحة عمل وأكبر قدر ممكن من التبريد.
2. يجب أن تكون الأبواب 106سم «إلى 122سم « عرض، و 200سم ارتفاع «
3. يجب أن لا تحتوي على نوافذ (من أجل الأمن والصوت والعوامل البيئية الاخرى كالأتربة والغبار
4. يجب أن تكون الارضيات من مواد مانعة للتشويش والكهرباء السّاكنة.
5. يجب أن تكون الجدران والسقوف عازلة للصوت.

Equipment
الأجهزة والمعدات:

1. يجب توزيع الأجهزة بحيث أقصى حمل هو 300 واط \قدم المربع.
2. يجب تأريض الراكات والأجهزة المتصلة.
3. توفير مساحه كافيه للراكات (120) سم من الامام (90) سم من الخلف (ولذلك لضمان عدم تحريك الراكات عند العمل عليها.
4. سقف الغرفة يجب أن لا يقل ارتفاعه عن 3 أمتار يجب توفر هاتف واحد على الاقل في الغرفة.

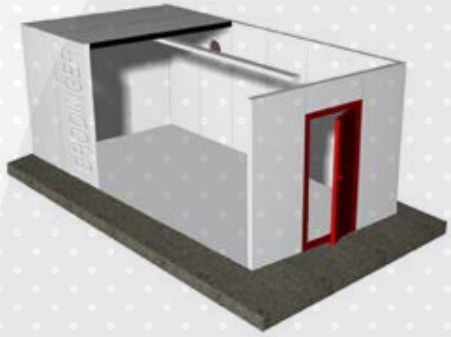
Fire prevention
الوقاية من الحرائق:

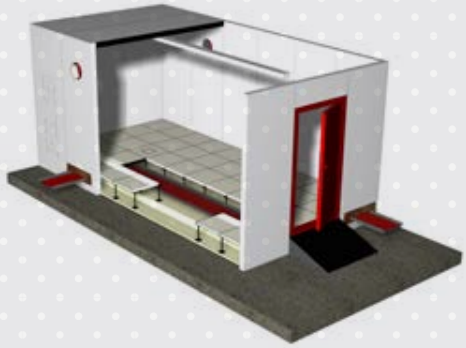
1. يجب أن تحتوي الغرفة على نظام إخماد الحرائق .
حيث يوصى بشده استخدام (""pre-action type system)
2. إذا تم الجمع بين الكابلات وأنظمة التبريد في نفس الفضاء فوق السقف أو تحت الأرض، يجب أن يكون للغرفة FIRE RATED.
3. يفضل استخدام نظام إخماد الحرائق الذي يعتمد على امتصاص الأكسجين من الغرفة.

COOLING SYSTEM

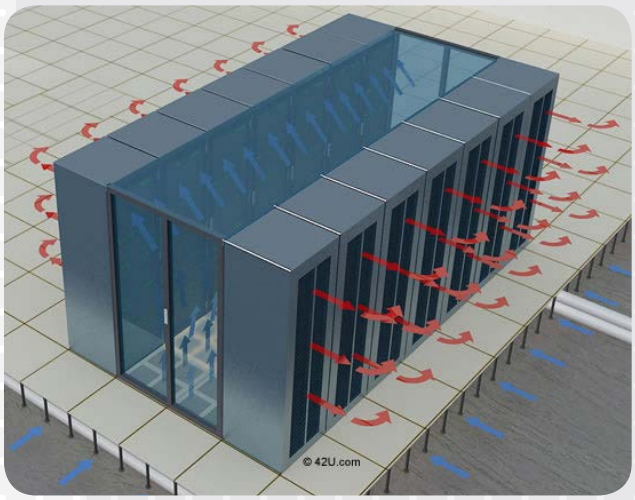
التبريد:

1. يفضل أن يكون نظام التبريد أرضي وذات توزيع منتظم حيث يساعد على دفع الهواء من الأسفل الى الأعلى وأيضًا أنظمة التبريد الأنبوبية مقبولة أيضًا.





2. يجب تقسم الراكات إلى أجزاء حار \بارد

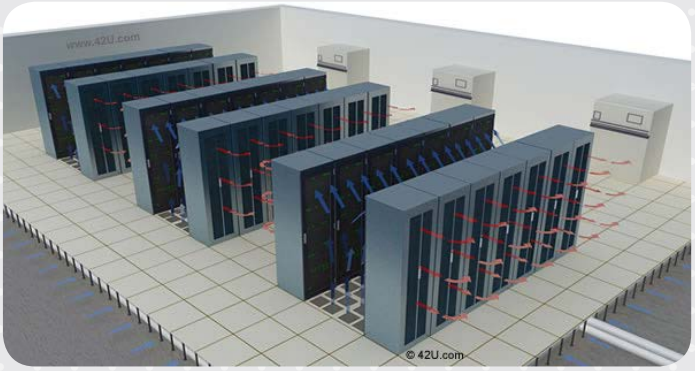


واذا كانت أنظمة التبريد تحت الأرضية يجب أن يكون أدنى ارتفاع هو 70 سم.
ويجب أن تكون مع أرضية قابلة لتحمل الوزن الكلي للراكات والأجهزة المستخدمة بالنّقل ووزن الأشخاص وأنظمة الدعم الأخرى.

MECHANICAL SYSTEMS

Air conditioning (AC)

بالنسبة لأنظمة التبريد حيث تعد من أهم مكونات الغرفة حيث يفضل نظام التبريد الأرضي الذي يعتمد على دفع الهواء من الأسفل إلى الأعلى ويجب تزويد الأرضية بدواعم .



1. أي نظام تكييف يجب أن يعتمد على الفريون (لا يعتمد على الماء مثل المكيف الصحراوي)
2. يفضل المكيفات السبلت عن المكيفات المركزية بسبب الأتربة التي تنتج عن الأخيرة.
3. يجب التحكم في درجة الحرارة والرطوبة داخل الغرفة بمكيفات، تكون منفصلة عن نظام التبريد الرئيسي للمبنى..
4. يجب تنظيم الراكات بحيث تحصل على التبريد الكافي فيما بينها.

- درجة حرارة الغرفة 22 درجة مئوية 2-+ درجة.
- درجة الرطوبة بالغرفة 45٪ -+ 5٪ ...
- يجب أن لا تقل المسافة بين المكيف والراكات عن 120 سم ... تفاديًا لأخطار تسرب المياه المحتملة، بالإضافة لإمكانية عمل صيانة للمكيفات دون الحاجة لتحريك الراكات.

FUTURE PLANNING

خطط المستقبل:

1. تصميم الغرفة يجب أن يتضمن تخطيط مناسب لتصريف مكثف (الماء المتكثف) وحدة التبريد سواء عن طريق الجاذبية الأرضية «أنبوب» أو عن طريق مضخة.

2. لضمان التبريد الكافي، يجب الأخذ في عين الاعتبار تركيب وحدة تبريد احتياطية إضافية –إن أمكن-بمعنى زيادة عدد المكيفات بالتصميم عن العدد المطلوب بوحدة تكييف إحتياطية.

3. يجب الأخذ في الإعتبار في التصميم التوسعات المستقبلية وملائمتها مع مواصفات النظام الكهربائي.

4. خلال مرحلتي التصميم والتشغيل يجب على المسؤولين حساب العزل الحراري للغرفة وهي تعمل في الظروف الاعتيادية من الحمل الحراري وحجم الهواء ، وذلك من أجل التخطيط الوقت المسموح به بين تعطل أنظمة التبريد (سواء تعطل كلي أو جزئي) ، ومتى تصل الغرفة إلى الحد الأقصى لدرجة الحرارة.

5. ربما يفضل المسؤولين تركيب برامج وأجهزة آلية لإغلاق الأنظمة بناءً على عدّة عوامل داخل الغرفة (مثلا إنذار الحرارة ، إنذار الحريق ، مجسات المياه)

النظام الكهربائي:

1. عند تصميم الغرفة يجب مراعاة أن تكون الدائرة الكهربائية أو مصدر الطاقة معزول عن باقي المبنى
وأيضًا أن تكون للغرفة دائرة تحكم منفصلة يختص بتشغيل الخوادم والمكيفات.

2. يفضل عدم وجود أجهزة توليد الطاقة عند انقطاع التيار «UPS» وأجهزة تثبيت التيار داخل غرفة السيرفر؛ وذلك لأنها تولد الكثير من الحرارة بسبب وضعها بأمكان قريبة.

3. يفضل وجود وحدة توزيع الطاقة A Power Distribution Unit (PDU) layout مع وحدات مراقبة الطاقة power monitoring and UPS لكل راك على حدة.

4. يجب تصميم نظام كهربائي ذو أرضية معزولة وشبكة تأريض مناسبة.

التخطيط للطوارئ:

1. يجب أن لا ترتبط أجهزة الطاقة الاحتياطية بنظام المبنى ، بل تعتمد الغرفة على أجهزة منفصلة.

2. يجب توفر مصدر طاقة احتياطي.

3. يجب أن تكون إمكانية الوصول للوحة التحكم بالطاقة الخاصة بغرفة السيرفر سهلة الوصول اليها – من قبل المسؤولين عن الغرفة- في حالة الطوارئ والحاجة لفصل التيار.

ALARMS AND SECURITY

الإنذار و الامن :
Alarm systems

- يفضل توفير أجهزة إنذار... (المكيفات – مجسمات للمياه - الحرائق) ... يفضل أن يعطى الإنذار لكل من إدارة القسم (IT DEP) وإدارة المبنى.

Security

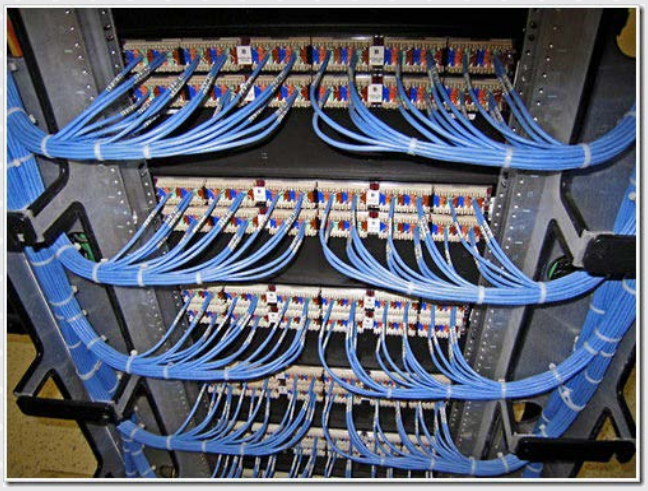
1. يجب تأمين جميع مداخل غرفة السيرفر جيدًا ، مع الإنذار عند الإقتراب منها.

2. يجب عدم السماح بدخولها لغير المخوليين وتحديد عدد المخوليين أيضًا مع صلاحياتهم.

3. يفضل وضع كاميرات مراقبة في الغرفة.

Ranking
الترتيب :

1. يجب عدم ربط الكيبلات بصورة مباشرة بالراكات أو الراوترات والسويتشات أو hubs وإنما باستخدام Patch panel.



a. حيث تقوم الـ Patch panel ، بحماية أجهزة الشبكة الأساسية والتي يتم الربط إليها من الصدمات الكهربائية ، ففي حال تسبب أحد الكوابل بحدوث تماس كهربائي ، فإن الصدمة ستصيب الـ Patch panel ، وبالتالي تحمي الجهاز الأصلي راوتر مثلاً ، والذي يمكن أن يكون ثمنه مئات بل ربما آلاف الدولارات.

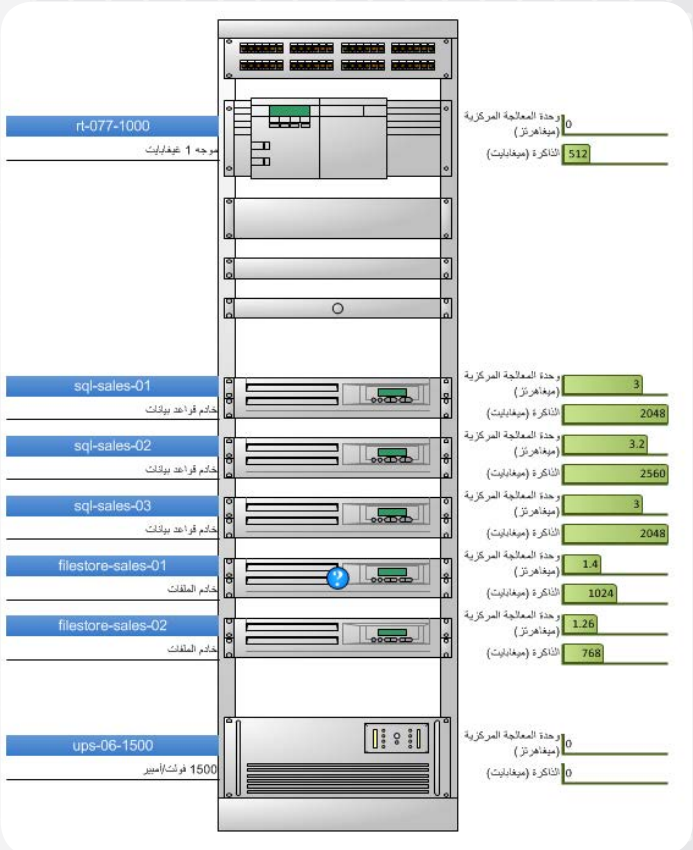
b. كما وتحمي أجهزة الشبكة الأساسية من أخطاء التركيب من قبل الفنيّين ، فمثلاً إذا قام أحد الفنيّين الموجود في غرفة أخرى ، بشدّ أحد الكوبل بقوة كبيرة ، فلن يتسبب في تلف ذلك الجهاز ، إنما سيتلقى الـ Patch panel الصدمة ويحميه.

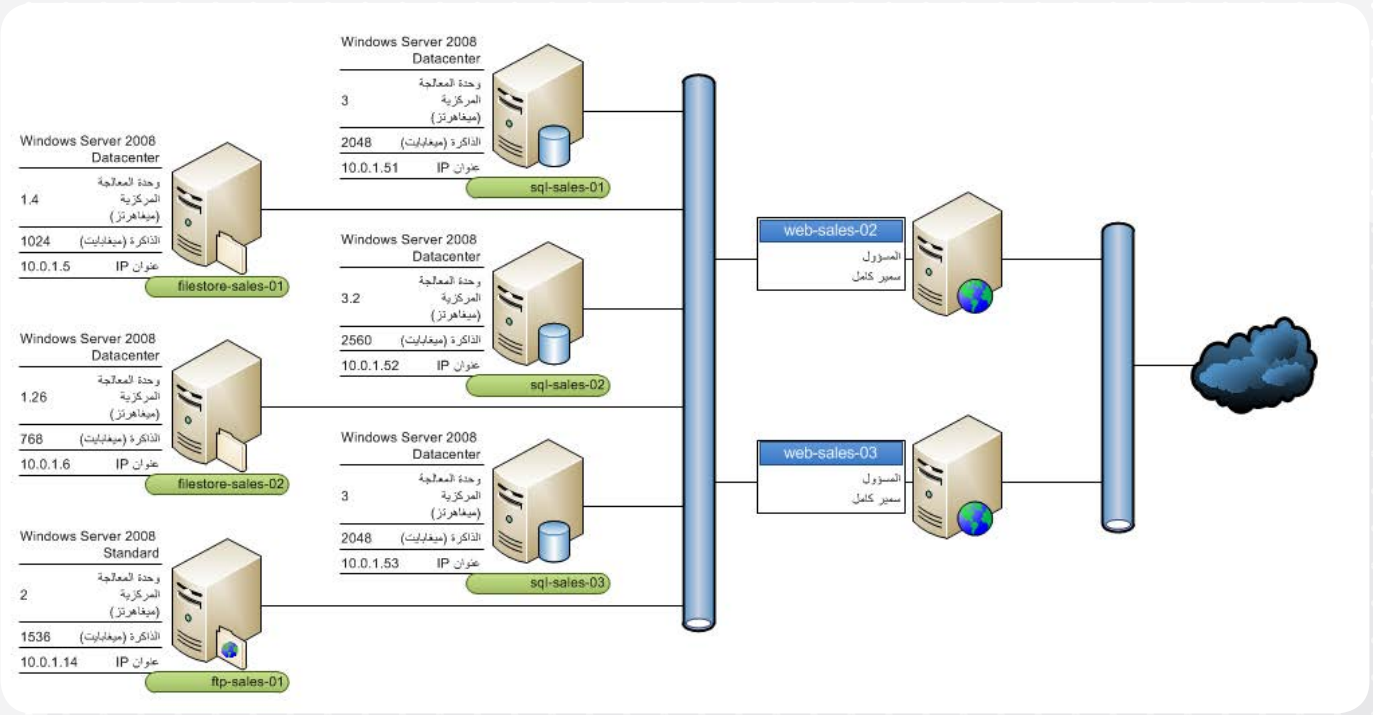
c. فائدة أخرى مهمة قد يستخفّ بها البعض أنه يمكن أن تقوم بالتعريف عن الأسلاك عن طريق الـ lable الموجود على الـ Patch panel ، بينما لا يمكنك ذلك في الأجهزة الاساسية أو بإلصاق الطوابع على الكوابل ، مما يساعد على تنظيم وترتيب الشبكة ، ويسهل التعامل معها .

2. محاولة ترتيب الأجهزة والرّاكات بصورة عملية ومنظمة (مثلا لو كان لدينا بناية شركة وتوجد فيها شبكتان واحده داخلية والأخرى متصلة بالإنترنت يجب ترتيب أجهزة كل شبكة براك منفصل.

3. إعطاء تسميات للأجهزة مثلا Router 1 (R1) switch (S) manage switch (M) الخ .....

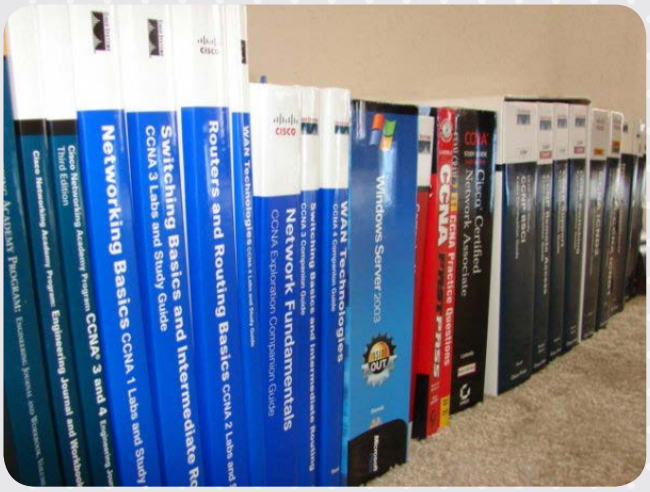
4. وضع رسم توضيحي للشبكة والأجهزة المستخدمة باستخدام أحد برامج الرسم (بالنسبة إلي استخدم MS VISIO 2010) حيث يساعدك المخطط على تحديد مشكلتك ومعالجتها.





5. تسجيل كافة الأعمال المنجزة خلال اليوم إذا كان أكثر من مسؤول في الغرفة وذلك لضمان معرفة الإجراءات وآخر التعديلات على الشبكة.

6. وجود بعض المراجع الأساسية وذلك اعتماداً على نوع الأجهزة المستخدمة MICROSOFT ,LINUX ,CISCO.



7. عدم استخدام الموبايل داخل الغرفة وذلك بسبب الترددات العالية الصادرة من الموبايل.

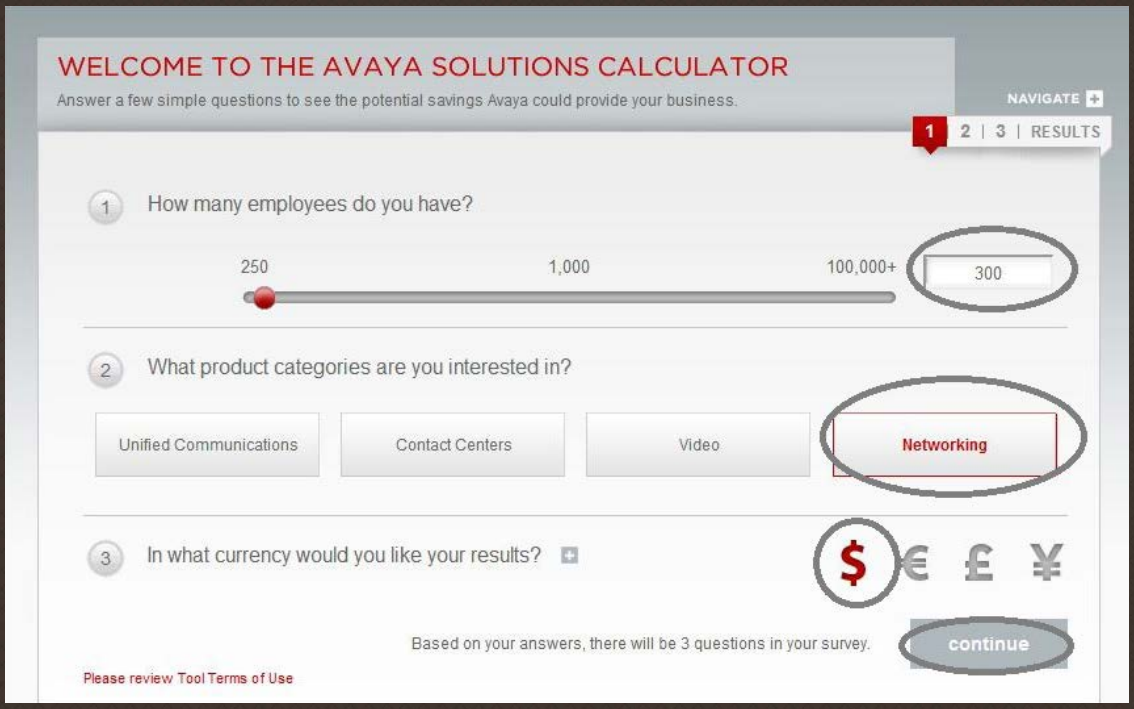
في هذه المقالة سوف نتعرف على أحد الـ online tools التى تقدمها شركة Avaya والتي قد ظهرت بقوةٍ في عالم الـ networks وخاصةً في مجال الـ VOIP ألا وهي Avaya Solutions Calculator.

ما هذه الـ tool وفيما تستخدم؟

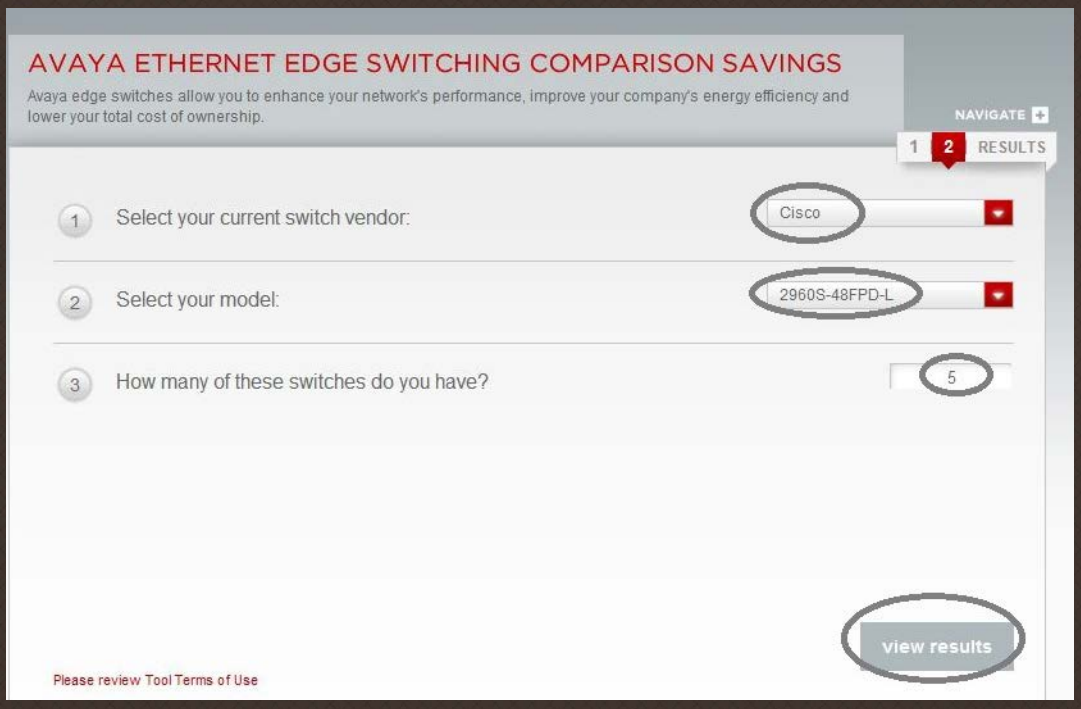
قدمت شركةAVAYA هذه الـtool في خطوة ذكية منها للمؤسسات والشركات، خاصةً في مجال الشبكات، حيث أنها تقدم لهم عرض في حال قامت أي من هذه المؤسسات باستبدال الـ network devices مثل الـ switches و الـ ip-phones من أي brand أخرى مثل ، HP ، cisco Juniper و غيرها التي لديها بالفعل الـ AVAYA Products ولها نفس الخواص و الإمكانيات، و تعرض أيضًا أمامك ما قد توفره من مال كخطوة إيجابية منها إلى التشجيع على التحويل للـ AVAYA Products .

نستطيع مشاهدة هذه الـ tool من خلال هذا الرابط .

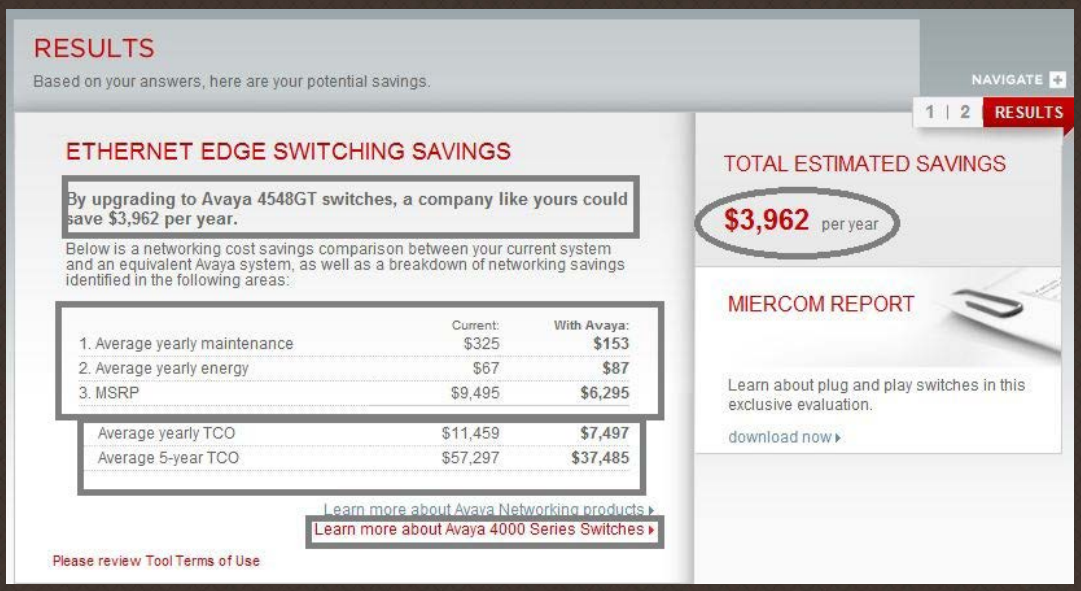
كما نرى أنها تسأل عن عدد الموظفين بداخل الشركة ، و تحديد ما هية نوع الـ devices التي تستخدمها لكي تعرض لك البدائل و النتائج فلنفترض أننا نمتلك عدد من الـ switches ونريد أن نرى ما سوف نوفره إذا قمنا بالاستغناء عنهم واستبدالهم بـ AVAYA Switches لها نفس الخواص والمهام، لذلك سنحدد من الـ product categories الـ Networking ثم نحدد عن رغبتنا بظهور النتائج بأي عملة، فمثلا سنحدد الدولار :



فى الخطوة التالية يُطلب منا تحديد نوع الـ products والعدد وكما اتفقنا أنها switches :



في الخطوة التالية سوف تُعرض النتيجة أمامنا ،يحدد لنا الـ avaya product
و يعرض ما سوف يتم توفيره سنويًا بصورة مفصلة مقارنة بالـ products الحالية لدينا و يتم عرض link فى حالة التعرف بالتفصيل على الـ avaya product البديل.



Identification
نادر المنسي
الجنسية : مصر / مقيم بالكويت
مهندس اتصالات يطمح و يساعد في الرقي بالمحتوي العربي للشبكات عبر ترجمة و اعداد مقالات و كتب علمية
naderelmansi@gmail.com
EGYPT

Cisco® Unified Wireless Network 7.2

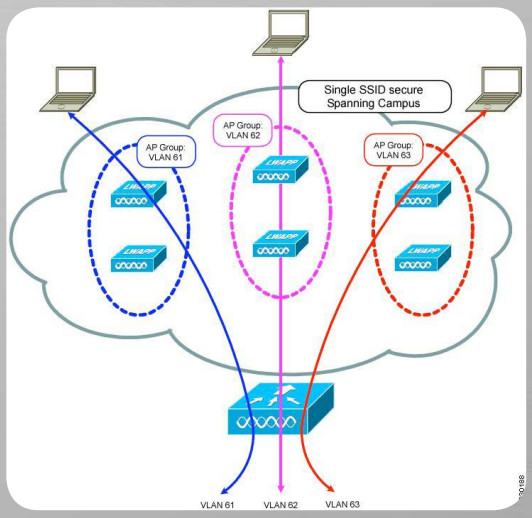
إنه الجيل الجديد من منظومة سيسكو التي أعدّتها للشبكات اللاسلكية بنسختها السابعة فاصل اثنين (7.2) و التي تسمى اختصارا CUWN 7.2 و التي قامت فيها بعمل طفرات جديرة في مجال الأمن و دعم الأجهزة المتنقلة المعتمدة على IP v6 و ذلك خلال العام الحالي 2012.

إن هذا الجيل الجديد هو أحد سلسلة سيسكو لجعل الشبكات اللاسلكية شبكات محورية و التي نستطيع أن نعتمد عليها بعيدًا عن الشبكات العادية أو على أقل تقدير إلى جانبها و ذلك عبر إيجاد طفرات في مجال الأمن و دعم IP v6 و استخدام أجهزة مؤتمرات الصوت و الفيديو، و لقد أعدت سيسكو في هذا الجيل جيشًا من الأجهزة و البروتوكلات و البرمجيات منها الجديد و منها المعدل مثل :

- Cisco Aironet access points running the Control and Provisioning of Wireless Access Point (CAPWAP) Protocol
- Cisco 2500 and 5500 Series Wireless Controllers
- Cisco Flex™ 7500 Series Wireless LAN Controllers (WLCs)
- Cisco Catalyst® 6500 Series Wireless Services Module 2 (WiSM2)
- Cisco 3300 Series Mobility Services Engine (MSE)
- Cisco Prime™ Network Control System (NCS) 1.1

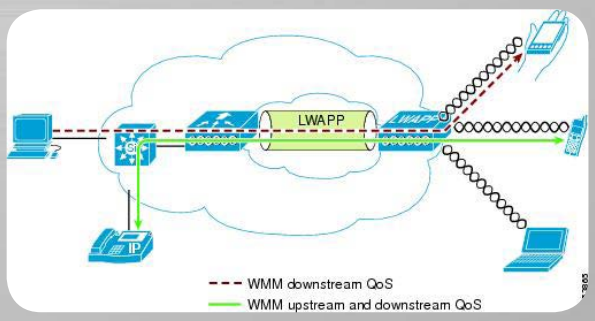
و سنقوم باختصار الخدمات التي اعتُمد عليها أو تم تطويرها في هذا الجيل .

AP Groups



و هي إمكانية عمل مجموعات افتراضية virtual من الأكسس بوينت طبقًا لنوعها أو مكانها أو أي معامل آخر و ذلك لتطبيق إعدادات معينة و يتم ذلك عبر تحكم مركزي من الكنترولر.

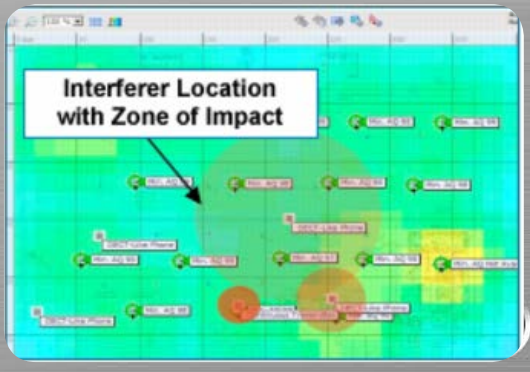
quality-of-service (QoS)



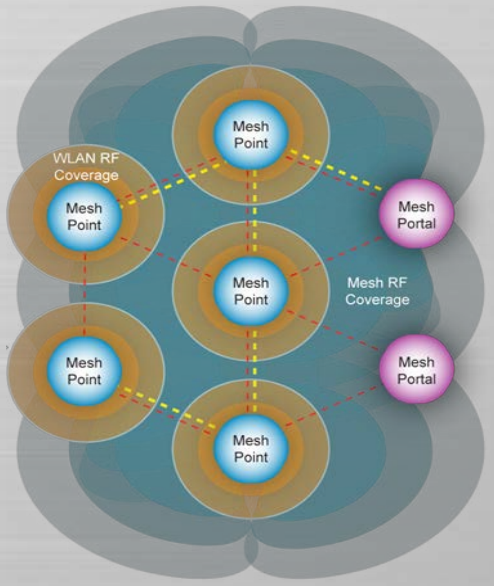
نستطيع تطبيق أولويات المرور في الشبكات اللاسلكية طبقا لتقنية QOS طبقا لـتدفقات Unicast و multicast للصوت و الفيديو و البيانات و هذا يتطلب أيضا تحسين نقل البيانات الآنية real-time multimedia applications عبر شبكات الوايرلس لتمكين عقد مؤتمرات الفيديو بواسطة تقنيات Video client scaling و Multicasting.

CleanAir™ Technology

تعتبر تقنية CleanAir من سيسكو من الأشياء الجديدة في سيسكو فعلى أساسها مثلا تقوم الأكسس بوينت و التي تعمل في وضع monitor Mode بجعل أجهزة الشبكة تتجاهل استخدام القنوات التي تعاني من تداخلات و شوشرة .

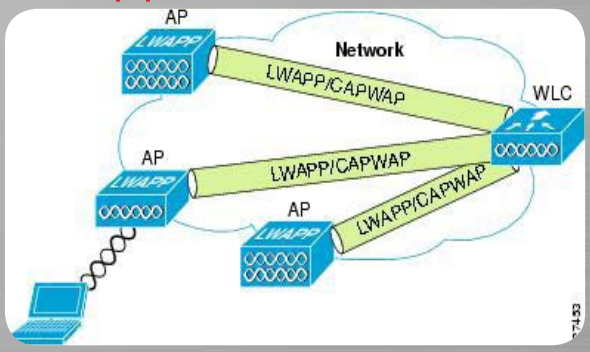


Indoor wireless mesh



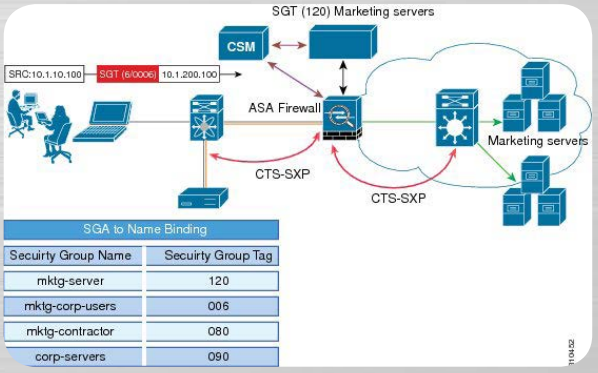
من المعروف أن الشبكات اللاسلكية المتشابكة Wireless Mesh قاصرة غالبًا على الشبكات الخارجية Outdoor إلا أن سيسكو بدأت في استخدامها في الشبكات الداخلية indoor و قامت بتحسين قدرات أجهزة الأكسس بوينت لهذا الغرض مثل Cisco Aironet 3600 Series access مع دعمه بتقنية 802.11n 4x4:3SS.

Support for CAPWAP



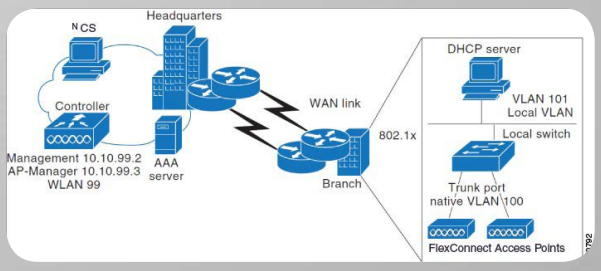
ظلت شبكات سيسكو تعتمد على البروتوكول LWAPP بين أجهزتها ثم بدأت بعد controller software release 5.2 باستخدام بروتوكول التراسل الجديد Control and provisioning of wireless access points CAPWAP و الذي يتيح للشبكة تحسينات في طريقة التواصل بين الأجهزة .

TrustSec®Security Exchange Protocol (SXP) support



من بروتوكولات سيسكو في أمن الشبكات عمومًا و قد استخدم مع CUWN في الشبكة اللاسلكية في إدارة و تطبيق السياسات الأمنية بشكل مركزي على مجموعات .

Cisco FlexConnect™



في الشبكات اللاسلكية يقوم كل أكسس بوينت بتحميل نسخته من الكنترولر و عند استخدام الكنترولر عبر شبكة wan فإن هذا الأمر قد يطول و يتأخّر، و في الشبكات التي نهتم بأمر السرعة فيها نقوم بتوظيف جهاز أكسس بوينت مركزي Master بتحميل نسخة نظام التشغيل من الكنترولر ثم يقوم بتوزيعها على باقي الأكسس بوينت في الشبكة و يسمى هذا الأمر FlexConnect™ و هو بروتوكول حصري لسيسكو.

Rogue enhancements

في النسخة الجديدة أصبح التحكم أكثر في الشبكة لمنع الأجهزة الدخيلة Rogue و ذلك بالتحكم في قيم شدة الإشارة RSSI received signal strength indication بل إن الشبكة أصبحت أكثر ذكاءً

وذلك بالتفرقة بين الجهاز الموصوف بصفة الإختراق و بين الجهاز المحتمل السماح بتواجده في الشبكة.

WI-FI Direct

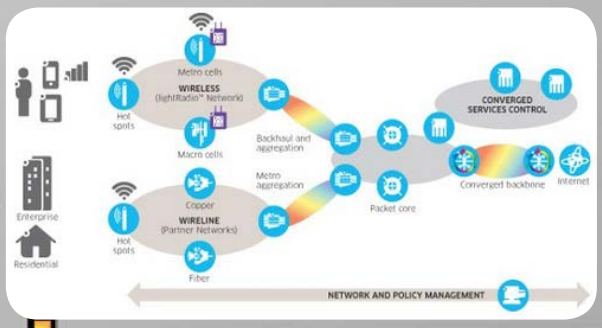
تم دعم التقنية الجديدة من معايير الواي فاي في سيسكو و المسماة WIFI-Direct و التي تسمح للأجهزة بالإتصال سويًا في وضع وسط بين Client-Client و Client-Server.

تعتبر هذه التقنية حديثة جدًا – تقريبا في عام 2010 – و من أحد اصدارات مؤسسة الواي فاي و هي تتشابه قليلا في الشكل العام مع تقنية Ad hoc و لكنها تختلف في المضمون معها و على العكس تتشابه في المضمون مع شبكات Infrastructure و تختلف معها في الشكل.

فالأجهزة التي تدعم هذه التقنية تستطيع الاتصال فيما بينها طبقًا لوجود مكون إضافي بها و هذا المكون ليس هاردوير بل سوفت وير يسمى "soft Access Point" أي أن الجهاز سواء كان موبايل أو كمبيوتر أو طابعة أو كاميرا يستطيع التعامل كأكسس بوينت و يتصل بأي جهاز آخر به هذه الخاصية.

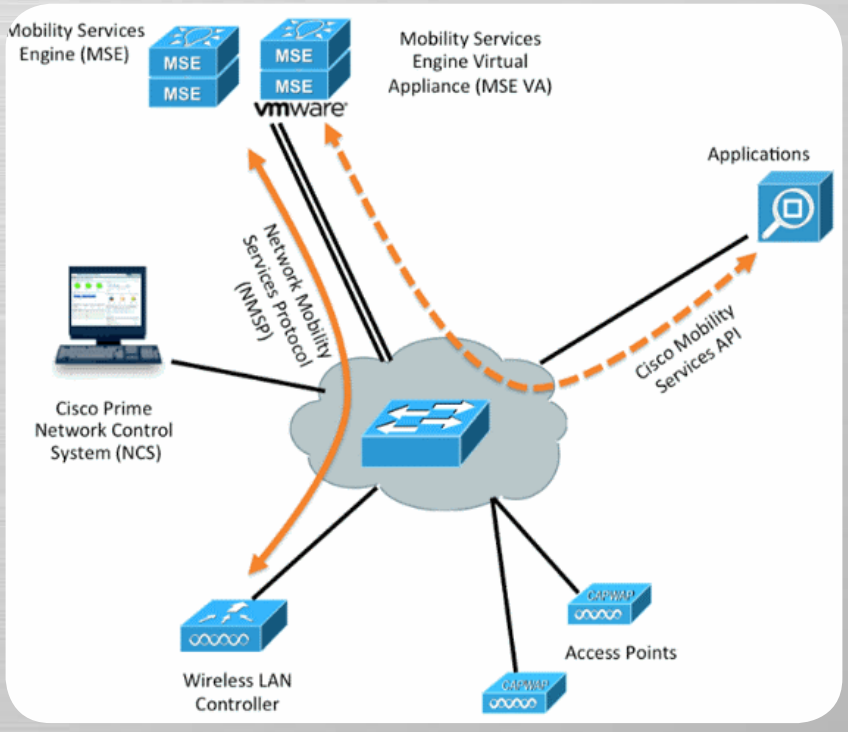
كذلك فإنها قادرة على تحقيق الإتصال عبر ترددات 2.4 و 5 جيجا هرتز على بعد 200 متر و بسرعة بمقدار 250 ميجابت في الثانية , في حال دعم الجهاز لمعايير تسمح بهذه السرعة مثل IEEE 802.n و كذلك فإن الأجهزة التي تدعم هذه التقنية قادرة على مشاركة الإنترنت للأجهزة المتصلة بها.

Next-generation hotspot 2



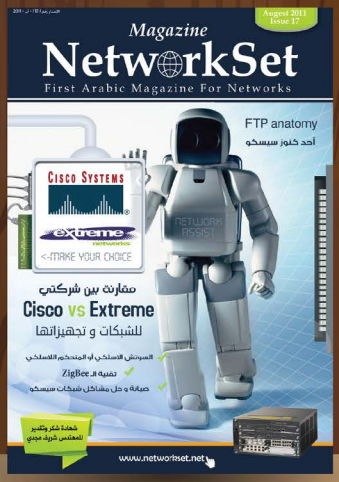
قامت سيسكو باستخدام وتطوير معيار 802.11u لتحسين الاتصال بشبكات الإنترنت المعدة للاستخدامات العامّة و المسماة hotspot و استطاعت أن تمكن هذه النقاط من تتبع الأجهزة و معرفة أماكنها بواسطة دعم تقنية GPS coordinates .

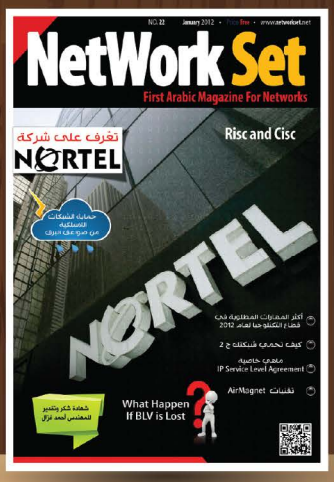
MSE Virtual appliance

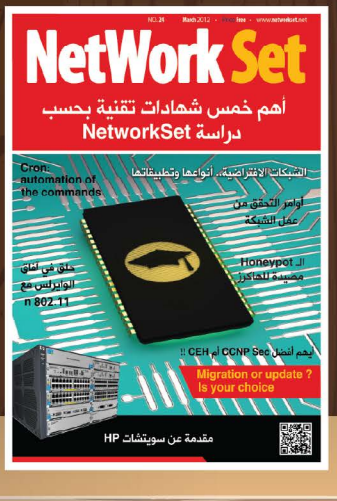


خدمات سيسكو المتنقلة للشبكات اللاسلكية MSE Mobility Services تم دعمها بقوة في CUWN 7.2 مع تطويرها كي يتم بناؤها على أنظمة افتراضية مثل VMware ESX و ESXi 4.1 hypervisor باستخدام نسخ OVA image و ذلك لتوفير استخدام أجهزة حقيقية.

Network Set Magazine Gallery







خدمة RPC

هل سبق وذهبت الى الشركة في أوقات متأخرة لتفقد بريد الشركة الدخلي (Exchange) لأنك تنتظر بريد مهم ويجب عليك متابعته ؟

هل سبق وتم توظيف أشخاص مهامهم فقط هي المتابعات البريدية ؟

إجابة هذه الاسئلة هي حديث مقالتنا التي تسعى لأبقائنا على التواصل الدائم بشركتنا لأن معظم الشركات تعرقل بعض الأمور لساعات أو أيام لعدم موافقة بريدية مثلاً أو متابعة أمراً ما.

للشركات المتوسطة والكبيرة ووجود برنامج الإكسشينج سيرفر الذي أصبح عصب الشركات والنظام المهم في عمليات المتابعات ووتوثيق العمل بين الموظفين.

الـ RPC اختصاراً لـ Remote procedure Call وهي خدمة مرتبطة بوجود الأكسشينج سيرفر المسؤول عن إنشاء نظام بريدي داخلي في الشركات (إرسال واستقبال الإيميلات بين الموظفين داخلياً وخارجياً)

تضمن الخدمة وصولنا للبريد الداخلي من خارج الشركة واستعراضه كاستعراضنا لبريد الهوتميل أو الياهو أو أي نظام بريدي خارجي .

مبدأ عمل الخدمة يعتمد على الأمور التالية :

1 - امتلاك أي بي ثابت (Static IP) : وهو الاي بي الذي من خلاله يتم تميزنا للعالم الخارجي (الانترنت) وتثبيته على راوتر الإنترنت لأنه في معظم الأحيان عند اشتراكنا بخط إنترنت يتم إعطائنا أي بي متغير (Dynamic IP) وبهل الحال لانستطيع استخدام أي خدمة موجودة داخل الشركة من الخارج إلا اذا دخلنا بموضع الـ Dynamic Dns

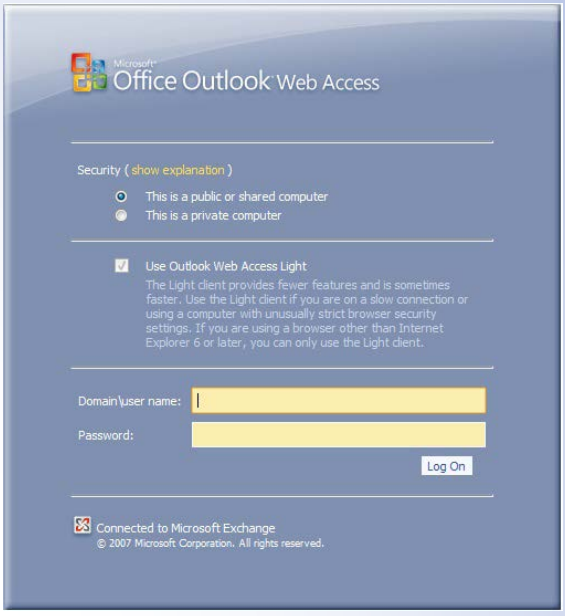
2 - إسناد الأي بي الثابت لأسم من أجل سهولة دخول الموظفين الى العنوان مثال :
ليكن امتلاكنا للأي بي التالي : 82.144.18.148
سوف يواجه صعوبة الموظف بحفظ أي بي وليس من المثالي كتابة أي بي في متصفح الإنترنت لذلك نذهب الى شركة استضافة تم التسجيل بها أو مجانية ويتم إنشاء DNS (A) Record يعمل على إضافة اسم وتحويله الى أي بي ليصبح كالتالي :
عند كتابة العنوان التالي :
https://RPC.networkset.net
يتم التحويل الى 82.144.18.148
أي الى راوتر الإنترنت في الشركة وبعدها الى السيرفر

3 - إنشاء شهادة (Certificate SSL) على السيرفر وتتم بشكل مجاني ولكن تتطلب بعض الإعدادات على سيرفر الدومين ليتحقق الوصول الآمن للبريد الالكترونيHTTPS

4 - تفعيل RPC من السيرفر (Feature) وهي يتم تفعيلها في ويندوز سيرفر 2003 – 2008

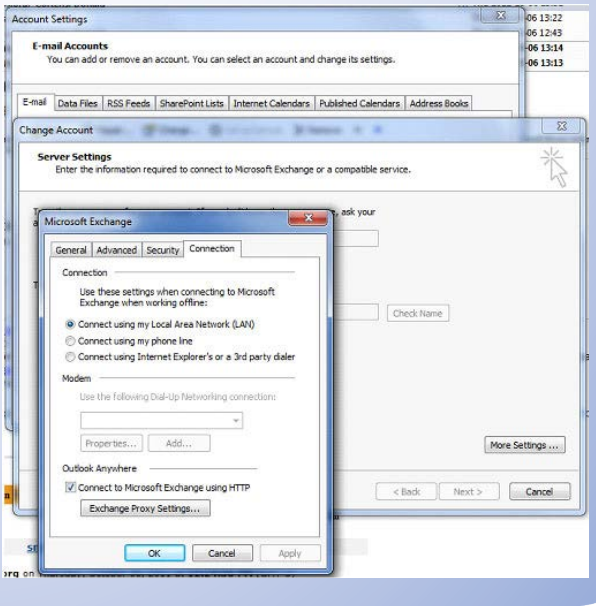
5 - وتفعيلها في برنامج الاكسشينج Enable OWA إن كان 2003-2007-2010 وربطه مع العنوان الذي تم إنشاؤه في شركة الاستضافة RPC.networkset.net
يتم استعراض بريدنا من الخارج على الطرق التالية :

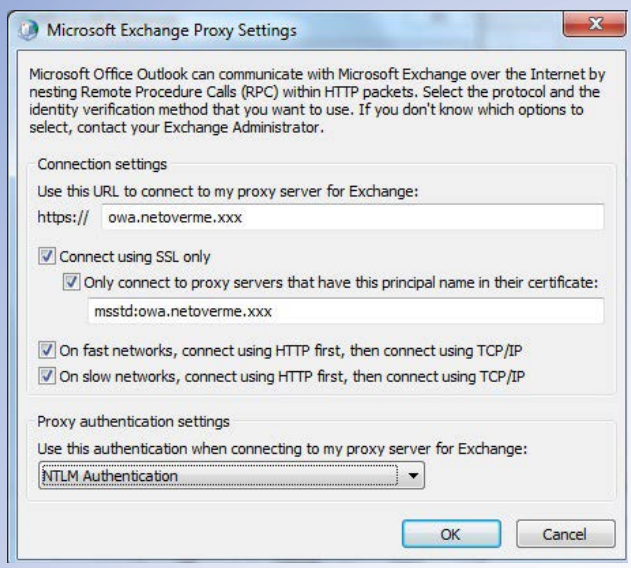
1 - طلب عنوان يتم تسجيله في شركة الاستضافة ويتم ظهور صفحة إنترنيت OWA (Outlook Web App) وبعدها إدخال اسم المستخدم وكلمة السر الخاص بي في الدومين (حساب الدخول الى الحاسب) وبعد ذلك يتم استعراضه كبريد خارجي على نمط الهوتميل أو الياهو كما ذكرت سابقا



2 - بعد تنزيل الشهادة (ملف تم إستخراجه من السيرفر حجمه صغير)على حاسوب خارجي أي ليس له علاقة بدومين الشركة أصبح بالإمكان تعريفه على برنامج الأوت لوك المعروف والوصول على حسابنا بضبط بعض الأعدادت في الأوت لوك .

مع ملاحظة : للموظفين الذين يملكون أجهزة محمولة وهم من ضمن الدومين (Join To Domain) يتم استدعاء الشهادة بشكل تلقائي من الدومين أي لاداعي لتنزيلها من أج الاستخدام خارج الشركة





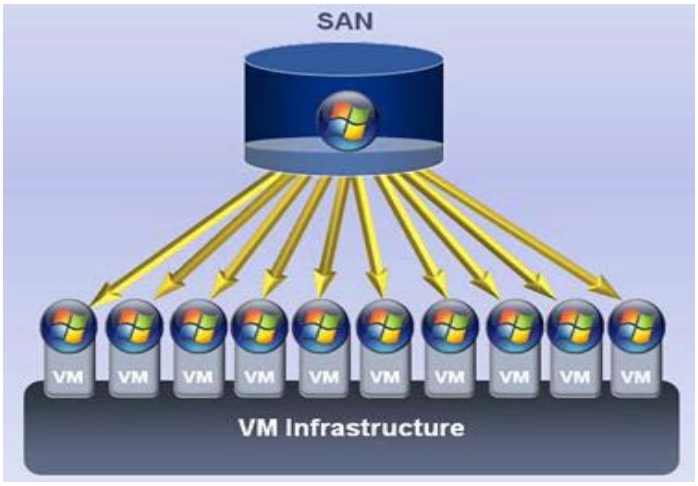
3 - إمكانية تعريف البريد الألكتروني عن طريق الهواتف النقالة الذكية مع اختلاف أنواع الأنظمة مثل
(Windows Phone –Android –IOS -) أو أي هاتف يملك الـ Active sync أو بوجود خيار في نظام تشغيل الموبايل وهو إضافة حساب إكسشينج جديد وبعدها وضع العنوان واسم المستخدم وكلمة المرور وبطريقة سلسة يتم إرسال واستقبال الإيميلات

ملاحظة : لأصحاب أنظمة ويندوز على الهواتف يجب تنزيل الشهادة بشكل يدوي ليس مثل الأنظمة الأخرى التي تعمل على استدعائها بشكل تلقائي

وبهذا الشيئ نضمن التزامن مع الشركة في الـ 24 ساعه وتساعد في تسريع عملية المتابعات التي تتعبر من أعمدة النجاح في الشركات

تكنولوجيا الـ
Virtual Desktop Infrastructure

الـ VDI أو Virtual Desktop Infrastructure ، أحد التقنيات التى تعد بمستقبل جديد ومختلف تماما عما عهدناه في عالم التقنيات, استخْدمتُ هذا الاسم لأنه الأشهر فى عالم الفيرجوال، وله عدة مسمّيات أخرى تبعًا للشرّكة التي تنتج برامج متخصصة فى هذا المجال.



دائمًا ما نقرأ عن كيفية تحويل السيرفرات الحقيقية إلى وهمية وهناك عشرات الكتب والمقالات التي تتحدث عن ذلك وأغلب الشركات التي دخلت مجال الفيرجوال قامت بذلك.

لكن موضوعنا اليوم يدور حول كيفية تحويل جزء مهم وضخم من الشبكة لدينا وهو تحويل أجهزة اليوزر إلى فيرجوال. ببساطة يتم تحويل الجهاز الخاص باليوزر من عمله على جهازه الحقيقي إلى VM تعمل على السيرفرات لدينا. وهذه الـ VM تحتوي على نظامه التشغيلي وعلى برامجه والدّاتا الخاصة به.

جهازه الحقيقي في هذه الحالة هو عبارة عن جهاز خالي من الداتا، فقط جهاز يستخدمه لكي يستطيع أن يتصل بال VM الخاصة به الموجودة على السيرفر . وهذه الأجهزة يمكن الاستغناء عنها أيضًا واستخدام أجهزة صغيرة الحجم تسمى Thin and Zero Client.

للتعرف على المزيد عن أجهزة الـZero and thin Client اقرأ هذا المقال فى الرابط التالي:

http://www.vmman.me/thin-and-zero-/client

بعض الذين يقرأون هذا المقال الآن سوف يقولون أن هذه التكنولوجيا قديمة أو أتت منذ زمن طويل، والبعض سيقول أنها عبارة عن ال Mainframe التى كانت تنتجها شركة IBM منذ 40 عام, أجيب عليهم أن هذه التكنولوجيا متشابهة مع بعضها فى بعض الأشياء، وتختلف أيضًا فى الكثير من الأوجه. تتشابه في أنها تمكّن أكثر من يوزر أن يستخدم نظام التشغيل أو البرنامج الموجود على السيرفر فى نفس الوقت لكن هناك نقاط اختلاف ضخمة بين الاثنين سوف تتضح لك بعد أن تقرأ المقال كاملاً.

ما هي الشركات التى تعمل فى هذا المجال؟

أهم ثلاث شركات تعمل فى هذا المجال هي:

1 - VMware (View)
2 - HyperV)+ Microsoft (RDP
3 - Citrix (XenDesktop)

وأيضًا العديد من الشركات الأخرى التي تقدم هذه التكنولوجيا لكنها محدودة وليست منتشرة. لذلك سوف نركّز على هذه الشركات وسوف نشرح بعض منتجاتهم فى مقالات مقبلة.

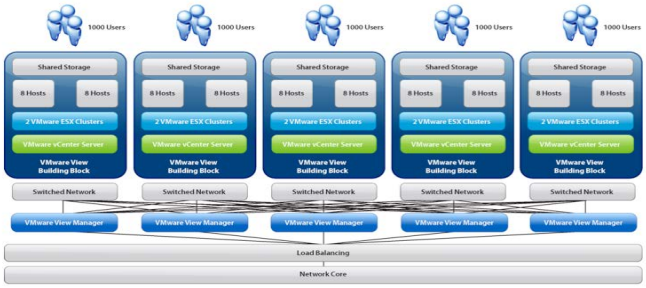
ما فائدة أن اليوزر يعمل على فيرجوال ماشين؟

يوجد عدّة فوائد من هذا الموضوع فى حالة عمل تصميم وتوزيع صحيح لها:

1 - أداء أعلى للـ VM الخاصة باليوزر لأنها تستخدم موارد السيرفر.

2 - حماية الداتا الخاصة باليوزر لأنها موجودة على السيرفرات ويتم أخذ نسخ منها على سيرفرات أخرى.

3 - عمل HA للماشين الخاصة باليوزر فى حالة أن السيرفر الذي يوجد على الماشين حدث فيه عطل.

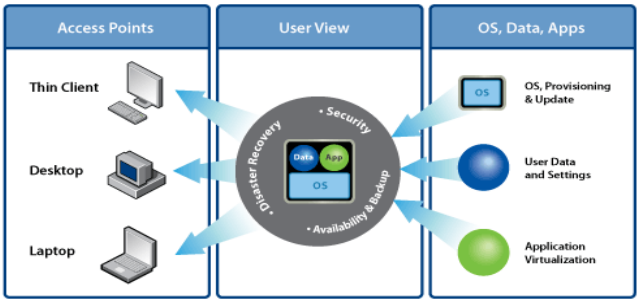


VMware View 5000 User Pod

4 - عمل ماشين لليوزر فى دقائق إن لم تكون خلال ثواني.

5 - عند حدوث مشكلة فى الويندوز الخاص باليوزر لا نحتاج لإعادة إعداد الويندوز والبرامج الخاصة باليوزر وإنما نقوم بعمل إعادة حالة الويندوز إلى حالته السابقة التي كانت تعمل عليها بصورة جيدة . أسلوب شبيه بالـ Snapshot بدون التأثير على الداتا الخاصة به.

6 - الحماية القوية على VM والداتا التي عليها لأن كل الداتا تكون على السيرفرات ولا يمكن سرقتها، وأيضا يوجد جدار ناري وأنتي فايروس يتم بناؤه حول هذه الماشين على مستوى السيرفر وليراقب كل الداتا الداخلة إلى الماشين التى تعمل على السيرفر والصادرة منها.



7 - الاستفادة من تكنولوجيا الـ Application Virtualization وهي أن اليوزر يمكن أن يعمل على برنامج ليس معد مسبقًا على الجهاز، أى أنه يعمل بشكل Portable من خلال برنامج الـ VMware ThinApp

يوجد مميزات كثيرة أخرى لهذه التقنية ولدينا عدة أساليب للعمل والاستفادة منها ويكثر فيها الكلام .

لكن أنا أقدم هذه المقالة كبداية للتعرف على التكنولوجيا وليس شرح كامل لكيفية العمل، لأن طريقة عملها ضخمة وتحتاج إلى تصميم ومعرفة متعمقة بتكنولوجيا الـ VT بكل تطبيقاتها.

ويوجد منهج وشهادات فى هذة الجزئية من شركات VMware – Citrix and Microsoft

فعلى سبيل المثال يوجد كورس لمدة 32 ساعة من شركة VMware وشهادة تسمى VCP-DT يحصل عليها المتخصصين فى هذه التكنولوجيا لمن يريد أن يتعرف أكثر والتعرف هذا الكورس يوجد شرح كورس VCP – DT كامل على الرابط التالي باللغة العربية:

http://www.vmman.me/vmware-view-/course

ملاحظة: لمن يريد أن يدخل هذا المجال يجب أن يدرس كورس الـ (vSphere) VMware VCP and VCenter

http://www.vmman.me/video-library/vcp-course/

****

نصيحة أخيرة : هذه التكنولوجيا سوف يكون لها مستقبل رهيب في الفترة القادمة وخلال سنوات قليلة من الآن سوف يتم تحويل أغلب أجهزة اليوزر إلى VM.

فقد أعلن فى أمريكا في العام الماضي 2011 أن الأجهزة الجديدة الوهمية التي تقوم الشركات بعملها لليوزر أكثر من عدد الأجهزة الحقيقية المشتراة، فالكل الآن يقوم بالتحول إلى هذه التكنولوجيا وهي تكنولوجيا شيقة للغاية وفيها حرفية عالية للغاية.

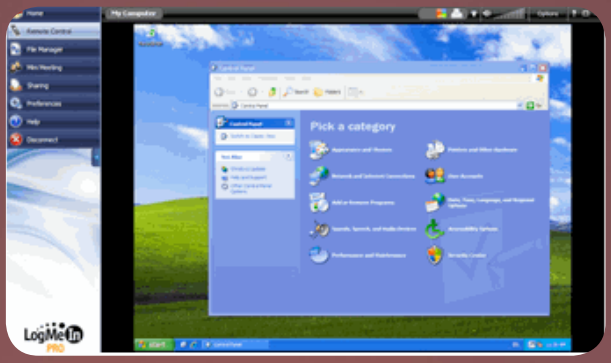
أفضل خمس برامج للتحكم بالاجهزة عن بعد

في مقالي لهذا العدد سوف أتحدث عن أفضل خمس برامج تستخدم للأتصال عن بعد أو مايعرف بي الـ Remote Desktop, وللموضوع أهمية كبيرة خصوصا عند فرق عمل الدعم والمتخصصين في إصلاح المشاكل أو الراغبين بالدخول إلى أجهزة بعيدة عنهم من أماكن مختلفة لمراقبتها أو أجراء تعديلات عليها.

Teamviewer

يعتبر برنامج Teamviewer من أكثر البرامج إستخداما في العالم لسهولة التعامل معه وتسطيبه على الجهاز وما يميزه عن غيره من البرامج أن الـ End user مهما كانت خلفيته في الكمبيوتر يستطيع التعامل معه, فبمجرد تشغيل البرنامج يتولد رقم خاص به عادة ما يتألف من تسعة أرقام يكون بمثابة العنوان الذي يمكن لأي شخص محترف أو تابع لأحد فرق الدعم إستخدامه للدخول إلى الجهاز وإصلاح المشكلة الموجودة. مميزاته كثيرة جدا وأهم واحدة أنه مجاني تماما ولا تحتاج إلى أي رخص. يمكن من خلاله تبادل الملفات وإجراء محاداثات كتابية أو صوتية, تستطيع التحكم بدقة العرض إعتمادا على سرعة الانترنت لديك أو لدى جهاز العميل بالأضافة إلى أنه آمن تماما ومشفر. يدعم الاجهزة اللوحية والأجهزة الذكية التى تعمل بنظام iOS وأندرويد.

LogMeIn



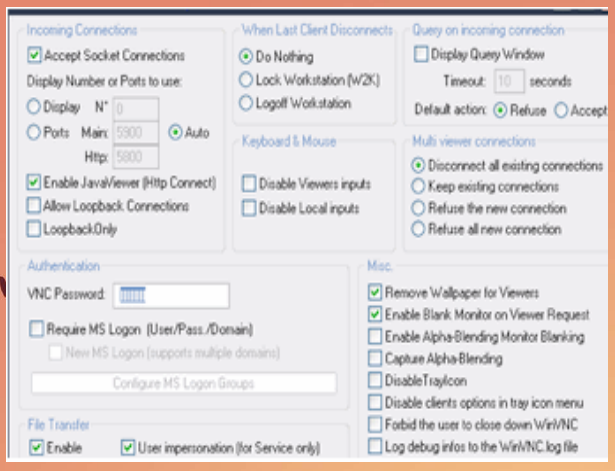
أحد البرامج التى حصلت على سمعة جيدة وبسرعة كبيرة, لهذا البرنامج نسختان, الاولى مجانية LogMeIn free و LogMeIn Pro كلا الاثنان يسمحان بالدخول عن بعد والتحكم بالجهاز لكن النسخة الأحترافية منه تقدم مميزات أكثر مثل تبادل الملفات ومشاركة الطابعة والـ Drug and drop ومميزات آخرى عديدة. مايعجبني في هذا البرنامج هو التحكم فمن خلال لوحة التحكم الموجودة على موقعهم تستطيع إضافة كل الاجهزة التى تتعامل معها وبضغة زر واحدة تدخل إلى أي جهاز وبدون حاجة إلى طلب أي شيئ من العميل فالبرنامج يعمل عند تشغيل الجهاز مباشرة. البرنامج يعمل على عدة أنظمة مثل الماك وويندوز وهناك نسخة لـ iOS. الميزة التى يملكها هذا البرنامج هي إستخدام المتصفح للدخول إلى اي جهاز موجود في القائمة لديك وقد سبق لي أن شاهدت أكثر من شركة تستخدم هذا البرنامج.

TightVNC

أحد البرامج المفتوحة المصدر التى تعمل على أنظمة مايكروسوفت ولينوكس يمكنك إستخدامه بشكل شخصي أو بشكل تجاري فمكن يتعامل مع برنامج التيم فيور بشل كبير يوميا سوف يجد مشكلة بخصوص هذا الأمر فالشركة سوف تعتبر عملك تجاري وسوف تطالبك بشراء رخصة لمتابعة العمل وهو ما يمنحك أياه هذا البرنامج فلو كنت من بين الأشخاص الذي تحتاج كثيرا الأتصال عن بعد أو تحتاج الاتصال بانظمة لينوكس فهذا البرنامج هو الأفضل بالنسبة لك, أثناء عملية التنصيب يجب مراعاة أختيار هل هذا الجهاز هو سيرفر أم عميل وسوفت تجد أثناء عملية التنصيب خيار للسماح للبرنامج بعمل أستثناء على الجدار الناري الموجود في أجهزة العملاء والتى قد نعاني منها أحيانا في بعض البرامج الآخرى التى تحتاج بعض الاعدادت على الجدار النري ليسمح للآخرين بالاتصال بالجهاز.

يسمح لك هذا البرنامج ايضا باستخدام المتصفح للدخول إلى الاجهزة لكن يحتاج منك تنصيب نسخة الجافا المخسسة للبرنامج.

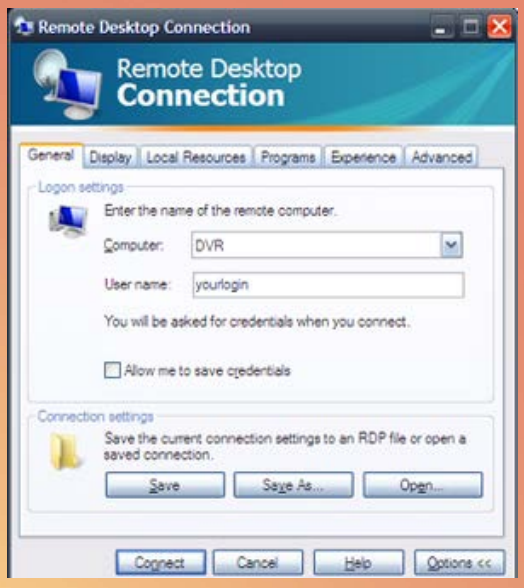
UltraVNC



أحد البرامج المفتوحة المصدر وهو خاص بمايكروسوفت فقط مجاني وفيه مميزات كثيرة جدا نقل الملفات والمحادثة والتشفير الذي ترغب به فالبرنامج يدعم الـ Plug-in ويمكنك إضافة التشفير الذي تريده, لم أجربه من قبل لكن بحسب ماقرات عنه فهو يستحق التجربة فعلى صفحتهم يتحدثوا عن أطنان من المميزات الموجودة مثل:

File transfer, Video driver, Optional Encryption Plugins, MS Logon, Text chat, Viewer Toolbar, Java Viewer with File Transfer , as well as Viewer Auto scaling and Server Side Scaling, Multiple-Monitors-support,Repeater/Proxy-support, Auto reconnection, good performances and tons of other functionalities,Repeater, SingleClick generator and NATtoNAT connectors.

Windows Remote Desktop Connection



أحد الادوات المعروفة والتى تأتي مدمجة مع أنظمة مايكروسوفت وخاصة بها فقط. أغلبها تعامل معها ويعلم مميزاتها مثل مشاركة الملفات والطابعة والتحكم الكامل بالجهاز لا تحتاج إلى أي برامج وكل ماعليك القيام به هو تفعيل الأداة على الويندوز من خلال الدخول إلى خصائص جهاز الكمبيوتر وتفعيل الجهاز. أحد البرامج المفضلة عند مديري الشبكات ويستخدم كثيرا في الشبكات الداخلية مع العلم أن هناك إمكانية لأستخدامه للاتصال بأي جهاز خارج الشبكة من خلال وجود أيبي حقيقية أو إستخدام خدمة الـ DynDNS أو أي خدمة آخرى مشابهة, لكن يحتاج في أغلب الأحيان عمل Forward على الروترات التى تتصل مع الانترنت للسماح لشخص خارج الشبكة بالدخول عن بعد.

هذه كانت أهم البرامج التى سمعت عنها وبالنسبة لي أستخدم الأول والآخير وسبق لي أن استخدمت LogMeIn لعدة مرات, هناك الكثير من البرامج التى تؤدي نفس الوظيفة لكن سمعت عنها وأنا أجري بحثي عن افضل البرامج مثل, Instant Housecall, Dimdim, ShowMyPC, Mikogo, Yuuguu , أغلبها يؤدي نفس الوظيفة مع بعض الأختلافات البسيطة, هذا مالدي لكم اليوم اتمنى أن تكونوا قد أستفدتوا من التدوينة ولو عند أحدكم برامج آخرى مفيدة فأرجوا أن تشاركونا إياها ودمتم بود.

شهادة WCNA

لا يكاد يخلو مجال في الشّبكات بما فيها شركات الـ IT والكورسات العمليّة للعديد من الشّهادات التّقنية وحتى تخصّص الشّبكات في الجامعات إلاّ وتكون هذه الأداة جزءًا لا يُستغنى عنه في ذلك المجال. وبحكم دراستي تعمّقْت في عمل هذه الأداة وبحثت في الإنترنت على كورس أو كتب تشرح هذه الأداة بالتّفصيل، فصادفت وتفاجأت بوجود شهادةٍ متخصصة بهذه الأداة الصّغيرة الاسم الكبيرة الفائدة والتي تمنح من قبل: Wireshark University وهي الشّهادة الوحيدة التي تصدرها هذه الجهة منذ عام 2007. الآن عرفتم ماهي هذه الاداة؟!

بالطّبع Wireshark فهي تعتبر من أهم الأدوات المفتوحة المصدر وصنّفت في المرتبة الأولى كأفضل أدوات السيكيورتي في مجال IT لعام 2010، حيث يصل عدد مرات التّحميل لها الى 500000 تحميل شهريًا. ولشهرة هذه الأداة لن اتطرّق إلى تفاصيلٍ أكثر عنها في هذا المقال، ولكن سوف سأدخل إلى تفاصيل الشّهادة الخاصة بها.

WIRESHARK®
CERTIFIED
NETWORK ANALYST

هذه الشهادة هي مختصر Wireshark Certified Network Analyst وتثْبتْ أنَّ حاملها قادرعلى استخدام Wireshark في مراقبة الشّبكة وتحليل الترافيك وتحديد المشاكل المتعلّقة بالأداء والسيكيورتي، كذلك فهي تثبت بأن حاملها لديه المعرفة بطرق الاتصال والبروتوكولات الخاصة بمجموعة TCP/IP واللازمة للقيام بعمله كمحلل شبكات.

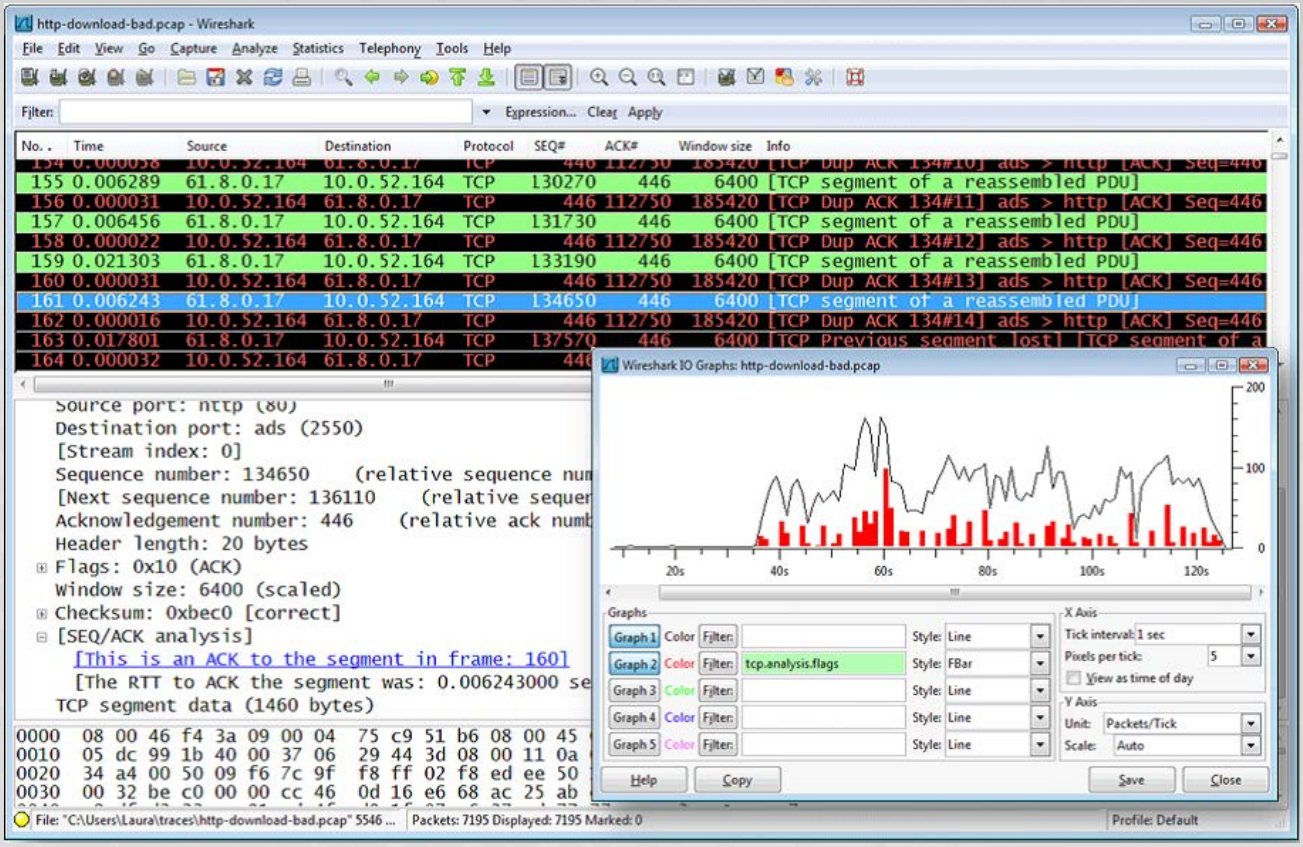
طريقة الحصول على الشهادة:

يمكن الحصول على هذه الشّهادة بعد اجتياز امتحان واحد أونلاين، إضافةً إلى اجتياز شرط، وهو الحصول على 20 نقطة أو ما تسمى CPE في العام الواحد (سأقوم بتوضيحها بعد قليل) ، ويتم معرفة النتيجة مباشرة بعد انتهاء الإمتحان. وعند عدم القدرة على اجتياز الامتحان في المحاولة الأولى يمكن إعادة المحاولة بعد مرور 5 أيام على تاريخ أداء الامتحان الأول ولا يحق للشّخص أداء أكثر من 3 امتحانات في السنة الواحدة.

نوعية الاسئلة والمواضيع المطلوبة:

فيما يتعلق بالأسئلة فتكون باللغة الانكليزية فقط وهناك نوعين من الاسئلة وهي: إما true/false أو الخيارات المتعدّدة Multiple Choice)) حيث يكون الجواب فقط تحديد اختيار واحد وليس أكثر من خيار كما في امتحانات الشّهادات الأخرى. وبعض الأسئلة تحتوي على صور لمخطّطات أو تفاصيل لباكيت معينة يتم السّؤال عنها، وتكون مدة الامتحان 120 دقيقة يمكن خلالها الرّجوع للسّؤال الذّي أجبت عليه وتغيير الإجابة. أما بالنّسبة للمواضيع المطلوبة في الامتحان فهي تنقسم إلى أربع عناوين رئيسية:

- Wireshark Functionality.
- TCP/IP Network Communications.
- Network Troubleshooting.
- Network Security.



المراكز والتكلفة:

نأتي إلى أهم نقطة في المقال وهي الأماكن التي توجد بها مراكز للامتحان، فهي تتواجد في غالبية الدّول العربية وللأسف لا يوجد لها مركز في العراق. وهذا رابط يحتوي على الدول التي لديها مراكز إضافة إلى عناوينها داخل الدّولة:

http://www.kryterionline.com/host_./locations

أما بخصوص تكلفة الامتحان فالسّعر حسب موقع الشركة على الإنترنت يبلغ 299 دولار، أما بالنّسبة للامتحان التدريبي فتكلفته 29 دولار. ويمكن التّسجيل للامتحان عن طريق الموقع التالي:

www.webassessor.com/pai ، ولمعرفة خطوات التّسجيل والتعليمات يمكن الاطّلاع عليها عبْر الموقع التّالي: www.wiresharktraining.com/certification.

صلاحية الشهادة:

الجزء الذّي يهم الكثيرين وهو فترة صلاحيّة الشّهادة، فهي تكون صالحة لمدة ثلاث سنين من تاريخ أداء الامتحان، وخلال هذه الفترة يجب على حامل الشّهادة الحصول على عدد نقاط لا يقل عن 20 نقطة أو كما يسمى CPE للتأكيد على أنك ما زلْت تحتفظ بالمعلومات التي اجتزت بها الامتحان.

الـ CPE هي نقاط تحصل عليها بعد القيام بأعمال أو نشاطات معينة في إحدى هذه المجالات:

- Network communications.
- Troubleshooting.
- Network testing/optimization.
- Network security.

وهذا مثال للنّشاطات المطلوبة بما في ذلك المدّة المطلوبة وعدد النقاط التي تحصل عليها:

Activity	Area	Duration (hours)	CPE credits
ONLINE TRAINING: Attend an online webinar about Wireshark	Network Testing/Optimization	2	2
TECHNICAL READING: Read RFC 1323 – Window Scaling and captured trace files for study	Network Testing/Optimization	2	2
CONFERENCE SESSIONS: Attend two Black Hat sessions focused on network forensics	Network Security	3	3
TECHNICAL READING: Read Wireshark Network Analysis Study Guide – Chapters 4-5	Network Communications	2	3

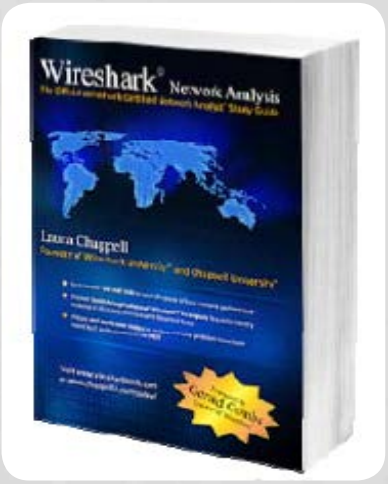
إضافةً إلى وجوب حضور مؤتمرات وندوات أخرى، وبعد ذلك تقوم بإبلاغ الجهة المانحة للشّهادة سنويًا بالفعاليّات التي قمت بها مع الاثبات.

الكورسات والمناهج:

تطرح الجهة المانحة للشّهادة فرصة التحضير للامتحان إما عن طريق الكورسات التدريبية، أو عن طريق التّعلم الذاتي.

لذلك، فهي تقدم كتابين أحدهما خاص بالمنهج المطلوب والآخر يقدم اسئلة تشابه تلك التي تصادفك في الامتحان.

الكتاب الاول:

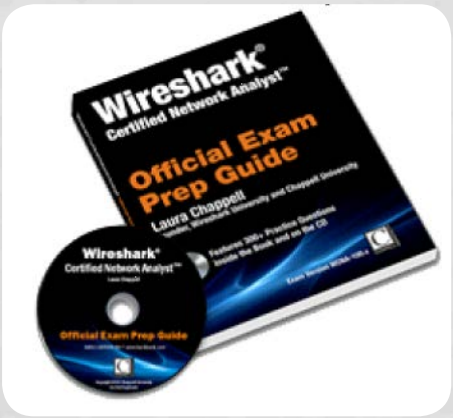


اسم الكتاب : Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide

عدد الصفحات : 800

وصف الكتاب : يغطي هذا الكتاب جميع المواضيع العلمية المطلوبة في الامتحان إضافة إلى المهارات الخاصة بعملية الـ Troubleshooting والسيكيورتي وغيرها، إضافة الى تقديم النصائح التي تساعد في اجتياز الامتحان.

الكتاب الثاني :

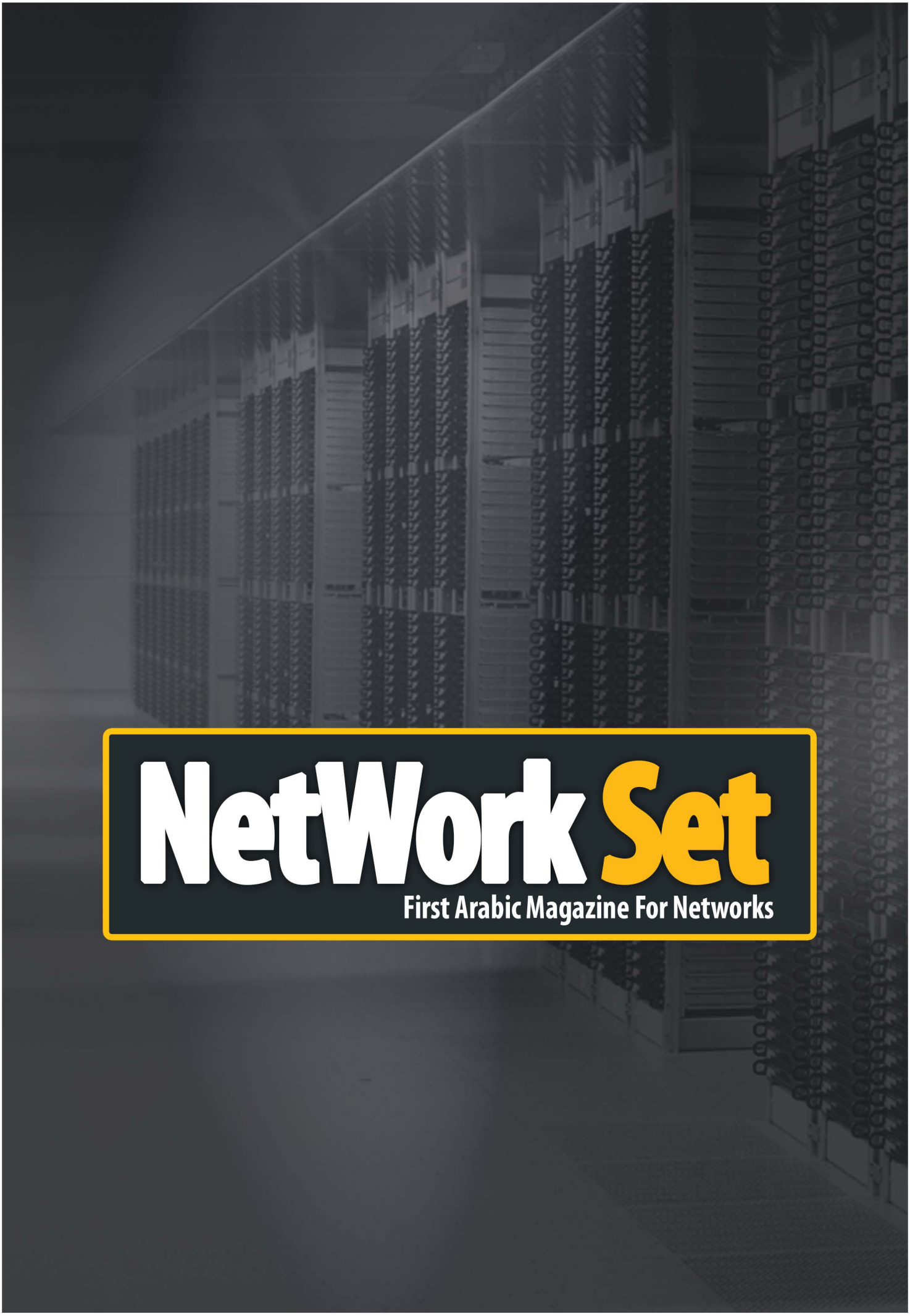


اسم الكتاب : Wireshark Certified Network Analyst: Official Exam Prep Guide

عدد الصفحات : 202 مع CD

وصف الكتاب : يحتوي على أكثر من 300 سؤال وتمرين، إضافة الى CD يحتوي على امتحانات تحضيرية تشبه الامتحان الرسمي إما محددة بوقت أو مفتوحة.

هذا ما حاولت تلخيصه في هذا المقال والشيء الجميل الذّي أعجبني في طريقة منح الشهادة هو نظام النقاط كونها تجعل حاملها في عملية تحديث مستمرة لمعلوماته، وحسب اضطلاعي فان بعض شركات الـ IT المتخصصة تعتبر إتقان العمل على هذه الأداة من الأفضليّات في التوظيف.



العودة إلى الفهرس